PATROL® Security User Guide

Version 1.2.01

August 16, 2002

bmcsoftware

Restricted Rights Legend

Contacting BMC Software

You can access the BMC Software Web site at **http://www.bmc.com**. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address	BMC Software, Inc. 2101 CityWest Blvd. Houston TX 77042-2827
Telephone	713 918 8800 or 800 841 2031
Fax	713 918 8000

Outside United States and Canada

Telephone	(01) 713 918 8800
Fax	(01) 713 918 8000

Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, please see “Before Contacting BMC Software.”

Support Web Site

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at **http://www.bmc.com/support.html**. From this Web site, you can

- read overviews about support services and programs that BMC Software offers
- find the most current information about BMC Software products
- search a database for problems similar to yours and possible solutions
- order or download product documentation
- report a problem or ask a question
- subscribe to receive e-mail notices when new product versions are released
- find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and e-mail contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at **www.bmc.com/support.html**.

Before Contacting BMC Software

Before you contact BMC Software, have the following information available so that Customer Support can begin working on your problem immediately:

- product information
  - — product name
  - — product version (release number)
  - — license number and password (trial or permanent)
- operating system and environment information
  - — machine type
  - — operating system type, version, and service pack or other maintenance level such as PUT or PTF
  - — system hardware configuration
  - — serial numbers
  - — related software (database, application, and communication) including type, version, and service pack or maintenance level

- sequence of events leading to the problem
- commands and options that you used
- messages received (and the time and date that you received them)
  - product error messages
  - messages from the operating system, such as `file system full`
  - messages from related software

Contents

List of Tables

About This Book

This book contains detailed information about PATROL® security components and is intended for system administrators. Use this book with the appropriate user guide for your console.

Note

This book assumes that you are familiar with your host operating system. You should know how to perform basic actions in a window environment, such as choosing menu commands and dragging and dropping icons.

How This Book Is Organized

This book is organized as follows. In addition, a glossary of terms and an index appear at the end of the book.

Chapter	Description
Chapter 1, “Introduction”	provides an overview of security concepts
Chapter 2, “Getting Started”	describes the PATROL security levels, configuration files, and instructions for loading and configuring PATROL Security features

Chapter	Description
Chapter 3, “Using PATROL Security Tools”	describes the PATROL security utilities available, and provides troubleshooting information
“Appendix A”	lists valid country codes for the Distinguished Name prompt “Country” as used by the sslcmd utility.

Related Documentation

BMC Software products offer several types of documentation:

- online and printed books
- online Help
- release notes

In addition to this book and the online Help, you can find useful information in the publications listed in the following table. As “Online and Printed Books” on page -xiii explains, these publications are available on request from BMC Software.

The following related documents are available for reference:

- *PATROL® Installation Guide*
- *PATROL® for Microsoft Windows 2000 Servers 2.1.00 Getting Started*
- *PATROL® for Microsoft Windows 2000 Servers 2.1.00 Release Notes*
- *PATROL for Microsoft Windows 2000 Performance Getting Started*
- *PATROL® for Microsoft Windows 2000 Server Performance Assurance Release Notes*
- *PATROL® Agent Reference Manual*

Online and Printed Books

The books that accompany BMC Software products are available in online format and printed format. You can view online books with Acrobat Reader from Adobe Systems. The reader is provided at no cost, as explained in "To Access Online Books." You can also obtain additional printed books from BMC Software, as explained in "To Request Additional Printed Books."

To Access Online Books

Online books are formatted as Portable Document Format (PDF) files. You can view them, print them, or copy them to your computer by using Acrobat Reader 3.0 or later. You can access online books from the documentation compact disc (CD) that accompanies your product or from the World Wide Web.

In some cases, installation of Acrobat Reader and downloading the online books is an optional part of the product-installation process. For information about downloading the free reader from the Web, go to the Adobe Systems site at **http://www.adobe.com**.

To view any online book that BMC Software offers, visit the support page of the BMC Software Web site at **http://www.bmc.com/support.html**. Log on and select a product to access the related documentation. (To log on, first-time users can request a user name and password by registering at the support page or by contacting a BMC Software sales representative.)

To Request Additional Printed Books

BMC Software provides a core set of printed books with your product order. To request additional books, go to **http://www.bmc.com/support.html**.

Online Help

You can access Help for a product through the product's Help menu. The online Help provides information about the product's graphical user interface (GUI) and provides instructions for completing tasks.

Release Notes

Printed release notes accompany each BMC Software product. Release notes provide up-to-date information such as

- updates to the installation instructions
- last-minute product information

The latest versions of the release notes are also available on the Web at **http://www.bmc.com/support**.

Conventions

The following conventions are used in this book:

This book includes special elements called *notes*, *warnings*, *examples*, and *tips*:

Note

Notes provide additional information about the current subject.

Warning

Warnings alert you to situations that can cause problems, such as loss of data, if you do not follow instructions carefully.

Example

An example clarifies a concept discussed in text.

Tip

A tip provides useful information that may improve product performance or make procedures easier to follow.

Note

Throughout this text, the **%BMC_ROOT** pathname variable refers to the installation directory.

- `All syntax, operating system terms, and literal examples are presented in this typeface.`
- In instructions, **boldface** type highlights information that you enter. File names, directories, and Web addresses also appear in boldface type.
- The symbol => connects items in a menu sequence. For example, **Actions** => **Create Test** instructs you to choose the Create Test command from the Actions menu.
- The symbol » denotes one-step instructions.

- In syntax, path names, or system messages, *italic* text represents a variable, as shown in the following examples:

  `The table table_name is not available.`

  system/*instance/file_name*

- In syntax, the following additional conventions apply:

  — A vertical bar (|) separating items indicates that you must choose one item. In the following example, you would choose *a*, *b*, or *c*:

  `a | b | c`

  — An ellipsis (. . .) indicates that you can repeat the preceding item or items as many times as necessary.

  — Square brackets ([ ]) around an item indicate that the item is optional.

- The following table shows equivalent mouse buttons for Unix users and Windows NT users:

Unix Button	Windows NT Button	Description
MB1	left mouse button	Click this button on an icon or menu command to select that icon or command. Click MB1 on a command button to initiate action. Double-click an icon to open its container.
MB2	not applicable	Click this button on an icon to display the InfoBox for the icon. To simulate MB2 on a two-button mouse, simultaneously press the two buttons (MB1 and MB3).
MB3	right mouse button	Click this button on an icon to display its pop-up menu.

Note

If you have a one-button mouse (such as an Apple Macintosh mouse), assign MB1 to that button. You should also define a user-selectable combination of option and arrow keys to simulate MB2 and MB3. For details, refer to the documentation for your emulation software.

Introduction

This chapter provides an overview of security concepts that will help you understand the issues involved in securing your PATROL environment. (To bypass conceptual information and start right away, you can go immediately to Chapter 2, “Getting Started”.) This chapter contains the following topics:

Overview of Security

All systems in any environment are susceptible to potentially harmful events if the proper security is not in place. Both internal and external users can instigate critical events, either maliciously or unintentionally. Careful implementation of security controls and restrictions minimizes the chance of security violations.

PATROL employs a security system that protects your PATROL environment with the options that you choose. You can install the level of security that you want and configure the chosen security level to your specifications.

Note

Throughout this text, discussion of PATROL security refers to the security employed by PATROL to address those security issues introduced by PATROL components; PATROL security is not intended to provide comprehensive network security.

Protecting PATROL Systems and Environments

Protecting data within PATROL means that the data delivered by PATROL users is private and secure. Once you install PATROL, the implementation of security within PATROL delivers the following:

- **Communications privacy and encryption.** PATROL security provides message privacy for communications between PATROL components.

- **Authentication.** Additional security is provided for communications between PATROL components by verifying the identity of PATROL consoles and agents.

- **Password privacy and configuration.** With password encryption inherent in PATROL, you can control and change encryption keys, thus helping to prevent unwanted access to your PATROL system environment. You can change your password to prevent infiltration of your accounts and to secure your personal environment and settings.

- **Digital signing.** To support the integrity of data that you create in PATROL, PATROL implements digital signing and verification tools. Signature verification proves that the signer's certificate is valid and was granted by a trusted certificate authority (CA). Once a signer's certificate has been verified, the certificate's public key is used for signature verification. The method of digital signature is only as secure as the signing keys that CA uses. Digital signing maintains the integrity of product-related files by helping to ensure that the PATROL Knowledge Module™ (KM) file or PATROL configuration file is original and unaltered. For more information, see “Trusted Root Authority Certificates” on page 1-15.

- **User privileges.** PATROL security administrators can define an account or group and can assign specific permissions and access rights to that user or group. As an administrator, you can add privileges to or remove them from a user or group of users.

- **Access control lists (ACLs).** To stop unwanted connections to a server running the PATROL Agent, the communication to and from the agents and consoles might require restricted access. PATROL ACLs specify which user names are granted access, from which hosts access will be granted, and what type of access will be granted to the PATROL Agent. Security administrators can manipulate the access control for any object in the PATROL namespace. Administrators can grant or deny access on a hierarchical basis for any object and for any user or group.

  In addition to ACLs maintained for PATROL consoles and agents, security level 4 also maintains its own set of ACLs. (For more information on security levels, see “Levels of Security” on page 1-7.)

- **Impersonation control.** To facilitate seamless functioning of PATROL across multiple hosts and security domains, PATROL incorporates an impersonation table, which a security administrator can use to specify user names and passwords for connecting to a new host.

For more specific information on how to use PATROL to modify or create these security functions, see the *PATROL® Agent Reference Manual*.

Types of PATROL Security

There are two major aspects of PATROL security: communications-level security and the administration of user rights and privileges.

Communications-Level Security

The term “security” covers a wide territory, even in the restricted domain of computer networks. Conventional log-in passwords, for example, ensure that only given to authorized users can access computing resources. Just as access security protects access to computing resources, communications security protects information that is transmitted over a communications channel.

Communications security protects such information only in the context of a transaction between communicating parties. Once that information is received, it moves from being a transaction requiring communications security into some other format (such as data stored on a disk), where it must be protected by other forms of security.

This book covers how security is implemented at the communications level. It discusses in detail the ways in which the transactions between PATROL components are secured so that message privacy is secured and the communicating components are authenticated. These two aspects of security (privacy and authentication) are addressed by communications-level security. Verification of the rights and privileges of communicating components (authorization) is addressed by user administration.

How Much Security Do You Need?

This version of PATROL introduces greater ease of use and more security options by offering five policy levels (the basic security level plus levels 1 through 4). These policies provide a predefined set of security configurations to choose from when you install PATROL.

The security policies allow you to install the least secure (basic security) up to the most secure (level 4) features of PATROL, depending on your system needs and how much complexity you can allow in securing your systems. High levels of security require additional configuration of the communicating components (the agent and console), are more difficult to use, and may affect network performance. Lower levels of security are much easier to configure and use, but provide less security.

Before installing PATROL, decide how much of a trade-off you are willing to make between security and usability by examining the differences between the five policy levels, as described in “Levels of Security” below. Basic security provides a minimal level of security with no configuration requirements. At the highest security level (4), all communicating components must authenticate with each other, and key databases must validate connection requests.

Note

All components in a system, including agents and consoles, must operate at the **same** level of security (basic, 1, 2, 3, or 4). This requirement is automatically ensured when you install PATROL with the basic (default) level of security.

Levels of Security

This section explains in detail the features of the five security levels. For a brief overview of the differences in security levels, refer to “Highlights of Different Security levels” on page 2-3.

Each security level is defined by a specific set of configuration variables residing in configuration files (as described in “PATROL Security Policies” on page 2-41). The following sections define the five principal levels of security policy.

Basic Security

Basic security is the default level of security employed when you install PATROL. This level offers the lowest level of security in exchange for greater ease of use. It is designated as security level “0” in the security configuration files.

Basic security provides authentication and protected password storage in unattended operations and only within PATROL (data from non-PATROL software is not secured).There is no cryptographic protection of network traffic and no product or data integrity. The PATROL consoles and agents communicate in clear text, which could expose the transferred data. Security and access control lists (ACLs) are minimized in favor of usability and performance. Digital signature verification failures are ignored.

Level 1 Security

Level 1 is based on the secure channel protected by an anonymous Diffie-Hellman public key exchange. A BMC Software proprietary protocol performs the exchange of the Diffie-Hellman public keys and triple data encryption standards-cipher block chain (DES-CBC) encryption to ensure privacy. Additional cryptographic services include communication channel privacy, integrity, and audit logging. As with basic security, PATROL ACLs are relaxed. There is no SSL authentication of the console or agent at this level.

Level 2 Security

Levels 2 and higher use Secure Socket Layer (SSL) protocol, the essential ingredient in providing high-level communications security in your PATROL environment. The agent provides a certificate to the console as part of the SSL handshake. The console accepts this certificate unconditionally—whether or not it can verify the certificate to a trusted root authority.

Because there is no SSL authentication of the console or the agent, the actual level of security is no higher than that of level 1. The difference lies in the use of the SSL protocol for message privacy. Level 2 defaults to unattended mode, allowing the agent to restart without requiring manual password entry.

Level 3 Security

Level 3 uses SSL protocol for message privacy. This level provides SSL authentication on the agent-side only. Level 3 security assures that the agent is not an imposter by requiring the agent to provide a certificate to the console, which must then authenticate the agent's certificate to a trusted root authority.The certificate of the trusted root authority must be present in the console's encrypted database. The console opens this database by supplying a password. Level 3 defaults to unattended mode, allowing the agent to restart without requiring manual password entry. You can configure level 3 to run in attended mode (see “How Higher Security Levels Affect PATROL Operations” on page 1-10).

Level 4 Security

Level 4 uses SSL for message privacy. This level provides SSL authentication of both the agent and the console. The agent and the console provide each other a certificate that proves their respective identities. Each certificate must be verified to a trusted root authority present in the agent and console databases. This level of security has the most configuration requirements and provides the most rigorous form of security available.

Level 4 defaults to unattended mode, allowing the agent to restart without requiring manual password entry. As with level 3, you can configure level 4 to run in attended mode (see “How Higher Security Levels Affect PATROL Operations” on page 1-10).

Password Requirements for Levels 3 and 4

Both levels 3 and 4 require a password to open the encrypted key and certificate database. The key database stores private and public key pairs, certificates, and trusted roots required for SSL operations. A DES-CBC cipher with a user-provided password protects the database.

A key material file computes the password encryption key. The key material file is a file that is provided and protected by the user and can be virtually any binary file. To ensure optimal security protection, users can carry this on their person, such as on a floppy disk. Chapters 2 and 3 provide detailed information on password encryption and policy definitions.

To allow higher usability of levels 2, 3, and 4, you have the option of storing the encrypted password in the configuration file (see “Unattended and Attended Modes” on page 1-11).

Summary of Costs and Benefits of Various Security Levels

The following table summarizes usability issues and configuration requirements for each of the 5 policy levels.

Table 1-1 Usability versus Security for the Five Security Levels

Security Level	Description
Basic Security	• Does not introduce any overhead in performance or configuration. • Does not provide any additional security beyond basic PATROL security features (see “Protecting PATROL Systems and Environments” on page 1-3).
Level 1	• Introduces a minimal amount of overhead associated with performance and disk space. • Introduces no overhead in usability or maintenance. • Provides only basic security such as traffic encryption.
Level 2	• Increases performance overhead and maintenance costs because of the use of SSL and X.509 certificates. • Pre-configured upon installation and does not require any additional configuration efforts.
Level 3	• Introduces SSL-based authentication and requires more configuration due to the requirement of a certificate for each authenticating agent. • Provides substantially increased traffic security and general data integrity.
Level 4	• Provides the tightest security measures by requiring a certificate for each authenticating agent and console. • Requires the most configuration due to the requirement of a certificate for each authenticating agent and console.

How Higher Security Levels Affect PATROL Operations

Installing security levels 3 and 4 affects PATROL operations in the following ways:

- Default operation for the PATROL Classic Console is operator mode.

- If you choose levels 3 or 4 during installation, an additional screen will appear and prompt you to select **TCP** and/or **UDP** for the **Network connection allowed** option. (For details on installation, see “Installing Security Components with PATROL and Selecting a Security Level” on page 2-6.)

  If you select the **TCP** option only, traffic defaults to TCP instead of UDP on the PATROL Agent. In order to use the **pconfig** utility at levels 3 and 4, you must specify pconfig ...+tcp to connect to an agent. (If you selected the UDP option, **pconfig** defaults to UDP).

  In order to use **xpconfig**, you can connect to the agent only by selecting the TCP connection mode.

Unattended and Attended Modes

A PATROL component operating in attended mode (available at levels 3 and 4) requires password entry to function; unattended mode allows PATROL to operate without password entry.

The presence or absence of password entries in the policy definition affect agent operations at levels 2, 3, and 4. When password entries are present in the policy files and registry keys, the PATROL Agent operates in the *unattended* mode. When the password is absent from the policy definition, the PATROL Agent script prompts you to enter a password for the key database for the PATROL Agent. On the console, you select a key database location and a password.

If password information is missing, the PATROL Agent operates in *attended* mode and requires a password. Therefore, you can make levels 3 and 4 agent operations more secure by removing the password entry from the policy definition. Attended mode is more secure than unattended operation using an encrypted password; however, attended mode requires you to enter a password every time you restart the agent.

The degree of physical security in your network environment is one factor to consider when deciding whether to run a server in unattended mode. A server that is not physically secured from unauthorized users is inherently more vulnerable to unauthorized access if it is running in unattended mode.

The following table shows the default mode for various PATROL components.

Table 1-2 Default Modes (Unattended and Attended)

PATROL Component	Default Mode (Security levels 3 and 4)
PATROL 3.x Console	Attended
PATROL Central - Microsoft Windows Edition	Attended
PATROL Central - Web Edition	Unattended
PATROL Agent 3.5 and 3.4	Unattended
PATROL Console Server	Unattended
PATROL Event Manager 3.5 PATROL CLI PATROL Link pconfig xpconfig wpconfig client apps	Unattended

To allow a component operating in attended mode to operate in unattended mode, a password with key material file, and the key database, must be specified as described in “Setting Up the SSL Key Database” on page 2-15. The password then resides in the policy file (Unix) or registry entry (Windows), as shown in the following example.

```
[client]
logfile = console_client.log
password =
82a153ecffbc901bb73fefe0c23c84b8b76d422a1e6ed83d,
/opt/Tuscany/JA/011016/common/security/keys/tree.bin
keyfile = /home/patrol/patrol.kdb
```

In the example above, a password (displayed above in its encrypted form), key material file, and key database file are specified for the PATROL Console in the console.plc policy file. (For more information on policy files and attributes, see “PATROL Security Policies” on page 2-41.)

To switch a component to unattended or attended mode, use the **plc_password** utility as described in “Using the plc_password Utility” on page 3-3.

Authenticated and Anonymous Communications

The level of security that you install determines whether or not the communicating PATROL components are authenticated with SSL communications security.

Basic security and levels 1 and 2 do not employ SSL to authenticate the communicating components. Levels 3 and 4 do provide SSL-authentication: level 3 authenticates the client to the server, and level 4 authenticates both the client and the server to each other.

Anonymous Communications

Security level 1 is based on anonymous Diffie-Hellman public key exchange, which provides a high degree of privacy protection but no authentication. Diffie-Hellman key exchange does not require any configuration and thus has no configuration cost and no configuration vulnerabilities. This protocol is a desirable choice for environments where only message privacy is required.

Security level 2 employs SSL for message privacy, but does not use SSL to authenticate the client or the server. Basic security (the default level) does not employ either Diffie-Hellman or SSL for message privacy. (For more information on differences between security levels, see “Levels of Security” on page 1-7.)

SSL-Authenticated Communications

Security level 3 employs SSL communications security to authenticate the server to the client (for example, the agent to the console). Authentication requires that a trusted third party, the certificate authority (CA), verify the agent's certificate. The integrity of this authentication process relies on the integrity of the key database that stores the trusted CA certificate.

Level 4 provides mutual client-server SSL authentication. This requires the proper maintenance of the authentication credentials on each of the communicating peers (clients and servers). For more information on differences between security levels, see "Levels of Security" on page 1-7.

SSL Communications Security

Security levels 2 and higher use SSL communications security for:

- message privacy (levels 2, 3, and 4)
- authentication (levels 3 and 4)

To provide communication security at level 2 or higher, you must set up an SSL key database for each user or PATROL component that presents or verifies certificates. To maintain communications security, an SSL key database contains:

- public and private cryptographic keys
- trusted authority certificates
- user certificates
- certificate revocation lists

PATROL components require a naming convention for both the key database filename and for the SSL identity that the database contains. To operate at levels 2, 3, and 4, the agent requires a key database named **server.kdb**, which must also contain an SSL identity named **server**. This identity provides the agent with its own keypair (one public key and one private key) and corresponding certificate.

The **bmcuser.kdb** file contains default keys and certificates for the agent and client with the default user name **bmcuser**. This setup enables PATROL security to run without configuration at level 3.

At level 3, the agent sends its certificate to the console for validation. The certificate contains the name of an issuer (the trusted root authority); the console searches for this name in the console database in order to verify the agent's authenticity. For more information, see "Trusted Root Authority Certificates" on page 1-15.

For level 4, the database must also contain an SSL identity key for the user name (for example, **user1**). This design permits a separate key database and password for each user. The console must provide its certificate so that the agent can verify the authenticity of the console. At this level, the console database must contain the signed certificate for the user while the agent database must also contain the certificate for the signing authority that signed the console's certificate.

To operate at security level 4, the SSL communications console requires a key database corresponding to the user name of the person starting the console. For example, **user1** requires a database named **user1.kdb**.

Note

To operate at level 4, **server.kdb** must contain certificates for all signing authorities that have signed the certificates of valid users. If multiple signing authorities sign user certificates, **server.kdb** must contain certificates for each of these signing authorities in order to grant all users access to the agent.

Trusted Root Authority Certificates

A certificate authority (CA), also referred to as the certificate signing authority (CSA), is a trusted public or private organization that validates digital certificates that, in turn, identify the source of online transactions. A certificate is validated by a hierarchy of CAs that approve the certificate. This process is called a "chain of trust." The final CA in the chain is called the "trusted root certificate authority" or "trusted root."

To operate at SSL levels 2,3, or 4, you must obtain a certificate authority certificate in your working environment. You can obtain the certificate of a trusted root from the CA that will be supplying the certificates. This digital certificate contains the authority's public key that you must use when requesting your product's certificate.

The certificates that you obtain must be an ASCII text file in version 3 of the X.509 PEM (Privacy-Enhanced Mail) Base64 format. The key database administrator utility (**sslcmd.exe**) uses the X.509 ASCII string format to import certificates. You can obtain these certificates with Microsoft Certificate Server, Netscape Certificate Server, and OpenSSL.

If you have a certificate in another format, you must obtain and use a translator program to convert the certificate to the X.509 Base64 format. For example, to convert a Microsoft certificate to an X.509 certificate, you would use the Microsoft INETSDK tools. For details on obtaining and converting certificates, see "Obtaining a CA Certificate" on page 2-34.

The following table lists the certificates required to enable various degrees of SSL security.

Table 1-3 Uses of Trusted Root Authority Certificates

For This Type of SSL Security...	Use This Certificate...
No authentication	No certificate necessary
Agent authentication	The trusted root for the SSL server
Console and Agent authentication	• The trusted root for the SSL server • The trusted root for the SSL client

Default Key Databases and Certificate Authorities

Warning

This product is delivered with default keys and certificates that are not unique to you. BMC Software highly recommends that you promptly change these default keys and certificates to ones that are unique. If you do not make these changes, there is a higher risk that any third party who gains physical access to your network, or to the data that you send over the internet, might have a better opportunity to use these default keys and certificates to gain unauthorized access to your system. BMC Software is not responsible for any damage or liability associated with your use of default keys and certificates.

Default keys and certificate authority (CA) certificates supplied by BMC and stored in keyfiles with .kdb extensions are provided only to demonstrate a turnkey security configuration, for purposes such as demos and trial installations. Before using BMC products, replace the default keys and certificates with your own unique entities. For instructions, see “Summary of Installation and Configuration Tasks” on page 2-5 and “Obtaining a CA Certificate” on page 2-34.

A password is required to open the default key files. The password for all default key files is **password**.

PATROL installs the BMC-provided default CA certificates in the key database in ..\common\security\keys. The default certificates will expire on the date specified in the certificate, as shown in the table below.

Table 1-4 Default Certificate Expiration Dates

Certificate	Expiration
server	Valid Begin: Thu Jul 19 21:15:54 2001 Valid End: Sat Jul 19 21:15:54 2003
bmcuser	Valid Begin: Wed Jul 25 12:27:21 2001 Valid End: Fri Jul 25 12:27:21 2003

Table 1-4 Default Certificate Expiration Dates

Certificate	Expiration
signer	Valid Begin: Fri Jul 20 06:32:48 2001 Valid End: Sun Jul 20 06:32:48 2003
WWWQA Testing Certificate Authority (CA)	Valid Begin: Thu Mar 25 10:44:14 1999 Valid End: Thu Mar 25 10:44:14 2004

Certificate Revocation Lists

Note

For information on installing a Certificate Revocation List (CRL), see "Installing a Certificate Revocation List" on page 2-31.

The validity of a certificate obtained from another party is determined by establishing a chain of trust for the certificate down to a trusted root certificate authority (CA). The purpose of the certificate is to provide the authentic value of the public key of another party. The chain of trust ensures that the value of the public key is true and not a forgery, and can therefore be safely used to verify the identity of another party or to encrypt data intended only for the other party. This chain of trust is secure only if the other party is the only one in possession of the private key to which the public key applies.

Revoking a Certificate

If the private key is given to an unauthorized entity or otherwise compromised, it should be invalidated through the use of a certificate revocation list (CRL).

The CRL is maintained by the CA. When the private key associated with the public key contained in the certificate is compromised, the owner of the compromised private key should immediately notify the CA that signed the certificate. The CA then publishes a CRL, which lists the certificate as having been revoked. Each user of a particular CA should obtain the CRL of that CA on a regular basis and install the CRL in the key database, so that if the revoked certificate is presented at a later date, the software will detect it as a revoked certificate and the chain of trust will be broken. If the Certificate Revocation List of a CA is missing from the key database, PATROL will issue the warning “REVOCATION UNKNOWN.”

Missing Certificate Revocation List Warning

The PATROL warning message “REVOCATION UNKNOWN” indicates that a chain of trust for a certificate has been established, but no CRL can be found for the CA. That is, the certificate is validated, but there is no list present to see if it has been revoked.

PATROL does not accept a missing list as meaning no certificates have been revoked. Only a signed CRL that is empty can accomplish this. PATROL does not regard “REVOCATION UNKNOWN” to be a fatal error. To prevent this message, install a CRL for the CA which signed the certificate, even if the list is empty.

Description of a CRL

CRLs are signed by the CA that issues them. The key database will not accept a CRL that has not had the certificate of the CA previously installed; therefore, a chain of trust for a CRL is established in the same manner as one for a certificate that is to be installed. A CRL is obtained from the CA by e-mail or over the web. In the PATROL environment, it is obtained in its Base64 encoding, as shown in the following example:

```
-----BEGIN CERTIFICATE REVOCATION LIST-----
MIIBVDCBvjANBgkqhkiG9w0BAQQFADB5MQswCQYDVQQGEwJVUzEOMA
wGA1UECBMFVGV4YXMxEDAO
BgNVBAcTB0hvdXN0b24xEjAQBgNVBAoTCUNvcnBvcmF0ZTEVMBMGA1
UECxMMQk1DIFNvZnR3YXJl
MR0wGwYDVQQDExRCTUMgU29mdHdhcmUgQ0EgUm9vdBcNMDExMDA0MT
kzNTQ3WhcNMDExMDA0MTk1
NTQ3WjAUMBICAQkXDTAxMDkxNzIxMDkzM1owDQYJKoZIhvcNAQEEBQ
ADgYEACh2SCmVhnnYXz95G
SHQ2WJbMBgjYkGvC4w/FF+c+4Q66ONbEZGmSFec3WfgW53Xb9C5RwK
SDwU3ORPYkH2yVhaUSDZkF
7M2AQdShu3K9fh3gs4pO1EBF/fOW4Frrc39w9fYML/3Jqp+9IOspJw
9Ymx3S0bub9Q+nnS6YofkM Up0=
-----END CERTIFICATE REVOCATION LIST-----
```

PATROL does not display the contents of the CRL. As new CRLs are issued by the CA, they are installed and overwrite any previous ones pertaining to that CA.

PATROL Knowledge Module Security

PATROL Knowledge Modules (KMs), along with configuration files, directly control the behavior of PATROL, and thus play an integral role in preserving the integrity of the PATROL user environment.

Because KMs require the PATROL infrastructure to deliver their functionality, KMs already include many security components that are handled by the infrastructure, such as traffic encryption, execution of the script in the proper accounts, and auditing. However, older KMs may offer less security.

Presently, all KMs use DES-encrypted storage in agent configuration. In addition, BMC Software is adding a set of basic rules for KM security that future KM development and certification processes will require.

Getting Started

This chapter provides highlights of the different PATROL security levels, supported platforms, and instructions for loading and configuring PATROL security features. The following topics are discussed in this chapter:

Highlights of Different Security levels

Before beginning installation of PATROL security, determine the level of PATROL security appropriate for your environment. The following table summarizes the key elements of each of the five levels of security available with PATROL.

Basic security (the default) is the lowest level of security. Levels 1 through 4 provide increasingly higher levels of security, along with increasingly greater configuration demands. For more detail on security levels, refer to “Levels of Security” on page 1-7.

Table 2-1 Highlights of Different Security Levels

Security Level	Description
Basic security	• Default level of security employed when you install PATROL • No cryptographic protection of network traffic • No verification of product or data integrity • Authentication provided and protected password stored in unattended operations in the PATROL application • Minimized security and access control lists (ACLs) in favor of usability and performance
Level 1	• Diffie-Hellman used for privacy • No SSL authentication of either party to the other
Level 2	• Private communications provided by SSL • No SSL authentication performed (console runs in keyless mode) • Defaults to unattended agent restart
Level 3	• Private communications and server authentication provided by SSL • Certificate provided by agent so that the console can authenticate the agent • Console not authenticated back to the agent • Defaults to unattended agent restart; can configure for attended agent restart
Level 4	• Private communications and mutual authentication of the console and the agent provided by SSL • Defaults to unattended agent restart; can configure for attended agent restart

Supported Platforms

For information on supported platforms, see the product-specific documentation for the product(s) you are installing. In general, the PATROL security components are available on the applicable supported platforms in Windows, Unix, and OpenVMS environments.

OpenVMS Directory Structure and File Locations

Throughout this document, instructions for Unix and OpenVMS are the same except as noted below. In particular, directory structures and file locations may differ between Unix and OpenVMS. For OpenVMS, the PATROL Security component files are organized as indicated in the table that follows. Note that the <*OS*> variable will equal **VAXEXE** or **ALPEXE** depending upon your operating system.

Table 2-2 PATROL Security Component File Locations

Filename	Path
patrol.conf	BMC$ROOT:[COMMON.PATROLD]
agent.plc esi.plc signer.plc verifier.plc site.plc	BMC$ROOT:[COMMON.PATROLD.SECURITY_POLICY]
dlls.conf	BMC$ROOT:[COMMON.SECURITY.CONFIG]
config.default	PATROL$HOME:[LIB]
sslcmd plc_password esstool *all other binary utilities*	BMC$ROOT:[COMMON.SECURITY.BIN.<*OS*>]
log files	BMC$ROOT:[COMMON.SECURITY.LOG]
access *key material file* key databases	BMC$ROOT:[COMMON.SECURITY.KEYS]

Summary of Installation and Configuration Tasks

After you have determined the appropriate security level, perform the following tasks to install and configure PATROL security. (Detailed steps are described in the sections that follow.)

Note

If you are installing PATROL for Microsoft Windows 2000 Performance, see *PATROL for Microsoft Windows 2000 Performance Getting Started* for installation information that is specific to the PATROL Performance product.

Table 2-3 PATROL Security Installation and Configuration Tasks

Tasks	For more information, see...
1. Install security components with PATROL and select a security level.	page 2-6
2. Configure the dlls.conf file.	page 2-10
Note: *The following step applies only if you are configuring SSL. Perform the following step only if you selected a security level of 2 or higher in Step 1.*	
3. Use the sslcmd utility to configure the key database.	page 2-12

Installing Security Components with PATROL and Selecting a Security Level

Summary: You will select a security level when you install PATROL. Note that all components in a single system must operate at the same level of security. Basic security (the default) is the lowest level of security. Levels 1 through 4 provide increasingly higher levels of security, along with increasingly greater configuration demands.

For general information on security levels, see "Highlights of Different Security levels" on page 2-3. For more detail on security levels, refer to "Levels of Security" on page 1-7.

PATROL security components are digitally signed using proprietary DSA keys. BMC Software recommends that you administratively protect any directories that contain PATROL security components.

Before You Begin

It is important to note the following requirements before beginning installation of PATROL security:

- It is recommended that you back up the **patrol.conf** and **config.default** files before installing security. Installation of the security components changes the information in these files.
- You must install the same level of security to all components within in a single client-server system.
- If you are installing PATROL for Microsoft Windows 2000 Performance, see *PATROL for Microsoft Windows 2000 Performance Getting Started* for installation information that is specific to the PATROL for Performance product.

On Unix only: If all of the following conditions apply, you must manually stop the agent before installing PATROL components, then manually restart the agent after installation:

- You are operating at security level 3 or 4 on a Unix agent *and*

- you are upgrading to a 3.5 agent from a 3.4.11 agent *and*
- you previously did an “over-the-top” installation of PATROL Security components on the 3.4.11 agent.

To Install and Select a Security Level

Step 1 Begin the PATROL installation process for the computers on which you want to install a particular security level. (See the PATROL installation guide for your platform for detailed instructions on installing PATROL.)

Step 2 When prompted, choose either the Typical or Custom installation as follows:

- If you want to install basic security (lowest level) you can choose either the Typical or Custom installation. The Typical installation path defaults to the basic security level.
- If you want to install security levels 1 through 4, you must choose the Custom installation.

Step 3 Click the **Next** button.

Step 4 If you chose the Typical installation, proceed as directed by the PATROL installation screens. Upon successful installation of PATROL, the security level is set to basic security (default level).

If you chose the Custom installation, the Select Level of Security screen appears and prompts you to select advanced security options. Proceed with the PATROL installation according to the steps that follow.

Step 5 On the Select Level of Security window, select one of the following options, then click **Next**:

- Advanced security options
- **Basic security (default)**

Note

If you plan on installing advanced security, BMC Software strongly recommends that you thoroughly review the contents of this user guide for information about the configuration requirements of each security level.

Step 6 On the Select Level of Security window, select **Yes** for the **Overwrite current security configuration (keys, certificates and trusted roots)?** option, then click **Next**.

Step 7 If you chose the default level of security, proceed as directed by the PATROL installation screens. Upon successful installation of PATROL, the security level is set at basic security.

If you chose the advanced security option, the Select Advanced Level of Security window appears. Select one of the following options, then click **Next**:

- **Level 1**
- **Level 2**
- **Level 3**
- **Level 4**

Step 8 If you chose levels 3 or 4, the Select Connection Type for Security window appears. Select one or both of the following options, then click **Next**:

- **TCP**
- **UDP**

Note

Installation of PATROL security installs the SSL keys and certificates that are specific to BMC Software. After you have successfully completed PATROL installation, configure your environment to use your own keys and certificates, as described in “Configuring the Key Database” on page 2-13.

Configuring the dlls.conf File

Summary: The PATROL for Unix OS KM for the PATROL Agent requires a file called **apidll.dll**. In order to load the **apidll.dll** file to the PATROL Agent, the **apidll.dll** file must be authenticated in **dlls.conf**. The **dlls.conf** file lists the .dll files necessary for KMs to work with the PATROL Agent.

The Unix OS KM begins collecting data from the PATROL Agent when the KM is loaded into a PATROL Console connected to the agent. Therefore, the **dlls.conf** file must be modified prior to loading the Unix OS KM into the PATROL Console so that all functionality of the Unix OS KM is available to the agent. After installing PATROL security components, perform the following steps to modify the **dlls.conf** file.

To modify the dlls.conf file

Step 1 At the command line prompt, change to the directory that contains the **dlls.conf** file:

- **%PATROL_HOME%\..\common\patrol.d** (Windows)
- **/etc/patrol.d** (Unix)

Step 2 Create the following entries in the **dlls.conf** file:

```
DLLDIR = $PATROL_HOME/lib/psl/$TARGET
DLL = apidll.dll
```

or

```
DLL = $PATROL_HOME/lib/psl/$TARGET/apidll.dll
```

Step 3 Specify any other dll files as needed:

```
DLLDIR = $<OTHER_DIR>
DLL = <otherdll>.dll
```

or

```
DLL = $<OTHER_DIR>/<otherdll>.dll
```

Step 4 Save and close the file.

Key Database Management

This section describes key database tasks you will perform using the sslcmd utility. For an example of screen shots you will see when performing these tasks, see “Example: Using the sslcmd Utility to Manage the Key Database” on page 2-32.

Using the sslcmd Utility

The **sslcmd** utility, located in **%BMC_ROOT\..\common\security\bin\<*OS*>** (Windows) or **$BMC_ROOT/../common/security/bin/<*OS*>** (Unix), is the command-line utility you use to manage the key database.

This utility displays a main prompt from which you can choose the following database management options:

1. Generate key
2. Add CA *(certificate authority)*
3. Generate CSR *(certificate signing request)*
4. List keys
5. Delete key
6. List certs
7. List CA
8. View CA
9. Add cert
10. Delete CA
11. Add CRL *(certificate revocation list)*
12. Change password
13. EXIT

Configuring the Key Database

After you install PATROL, use the sslcmd command to perform the tasks in the following table in order to configure the key database (perform only if you selected security level 2 or higher during installation). For an example of screen shots you will see when performing these tasks, see “Example: Using the sslcmd Utility to Manage the Key Database” on page 2-32.

Table 2-4 Key Database Configuration Tasks

Task	sslcmd option #	For more information, see...
1. Set up the SSL key database.	N/A	page 2-15
2. Install the root authority certificate in the key database.	2	page 2-17
3. Verify trusted root authority certificates.	7	page 2-19
4. Generate public and private keys for a certificate.	1	page 2-20
5. Create a certificate signing request.	3	page 2-22
6. Install a certificate in the key database.	9	page 2-24

Maintaining the Key Database

You can also use the sslcmd tool to perform the following non-configuration, maintenance tasks:

Table 2-5 Key Database Maintenance Tasks

Task	sslcmd option #	For more information, see...
List public and private key pairs in the key database.	4	page 2-26
List signed certificates in the key database.	6	page 2-27
View field information for CA certificates.	8	page 2-28
Delete trusted root authority certificates.	10	page 2-29
Delete private and public key pairs and certificate.	5	page 2-30
Install a certificate revocation list.	11	page 2-31

Transferring a Keyfile.kdb from a Unix Machine to a Windows Machine

If you set a keyfile.kdb using a Unix computer, you can use file transfer protocol (FTP) to transfer the file to a Windows computer. It is important to transfer the file using the **bin** command so that the file is transferred as a binary file rather than an ASCII file.

Setting Up the SSL Key Database

Summary: If you selected a security level of 2 or higher during the PATROL installation procedure, perform the following steps to set up your own SSL key database. For information on why setting up your own key database is recommended, see "Default Key Databases and Certificate Authorities" on page 1-17.

To Set Up the SSL Key Database

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

The following message is displayed:

```
File <keyfile.kdb> not found.
Enter new key file <keyfile> password (at least 8
characters):
```

Step 3 At the **Enter new key file <keyfile> password (at least 8 characters)** prompt, enter a password. The password must be at least eight characters and can be a combination of letters, numbers, or special characters.

Step 4 Reenter the password when prompted.

The system creates a new key database named ***keyfile.kdb*** and displays a menu that shows the actions you can perform with the key database file.

The database is now accessible only by using the password that you specified. (To change the password, use sslcmd option **12** for the **Change password** command.)

Note

BMC Software recommends that you back up your key database file on a regular basis and keep the backup copy in a secure location.

Step 5 Proceed to the task on the following page.

Installing a CA Certificate in the Key Database

Summary: If you selected a security level of 2 or higher during the PATROL installation procedure, perform the following steps to set up a certificate authority (CA) certificate in the SSL key database.

Before You Begin

Obtain a root authority certificate in the required format as described in "Obtaining a CA Certificate" on page 2-34.

Note

The CA certificate you are installing in this task differs from the public-private keypair certificate you install in "Installing a Keypair Certificate in the Key Database" on page 2-24

To Install a Root Authority Certificate in the Key Database

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 At the command line prompt, enter the password for the SSL key database file that you want to access.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **2** for **Add CA** to add a CA's certificate to the key database.

Step 5 At the **Enter CA certificate file name** prompt, enter the file name of the CA certificate.

Step 6 Copy and paste the CA certificate from the vendor site (see “Obtaining a CA Certificate” on page 2-34).

The system installs the specified CA certificate in the SSL key database and a verification message is displayed.

Step 7 Proceed to the task on the following page.

Verifying Trusted Root Authority Certificates

Summary: If you selected a security level of 2 or higher during the PATROL installation procedure, perform the following steps to verify the trusted root authority certificates.

To Verify Trusted Root Authority Certificates

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 At the command line prompt, enter the password for the SSL key database file that you want to access.

The system displays a menu that contains database commands.

Step 4 Enter **7** for **List CA** to see a list of the certificates installed in the key database.

A list of the certificates installed in the key database is displayed.

Step 5 Proceed to the task on the following page.

Generating Public and Private Keys for a Certificate

Summary: If you selected a security level of 2 or higher during the PATROL installation procedure, perform the following steps to generate public and private keys for a trusted root authority certificate.

Before you can request a certificate from the certificate authority, you must generate a public and private cryptographic key pair as described below. Next, assign that key pair to the new certificate for a BMC Software product user or product component. A cryptographic key pair is a set of two cryptographic keys (one publicly shared and one private) used to start an SSL session.

To Generate Public and Private Keys for a Certificate

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 Enter the password for the SSL key database file that you want to access.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **1** for **Generate Key** to generate a public/private key pair to be assigned to a new certificate.

Step 5 At the **Enter identity** prompt, enter an identity (alias) name for the key pair.

The identity name is the ID that identifies the public/private key pair. The identity is usually the same as the name of the key database file.

Step 6 At the **Enter keypair type, D for DSA, <other> for RSA** prompt,

- If you want to choose an RSA algorithm, press the **Enter** key. (recommended; supported by most certificate authorities)
- If you want to choose a DSA algorithm, enter **D**.

Step 7 At the **Enter key length 512|1024** prompt, enter the size for the public/private key pair that you want to create.

You can choose either a 512-bit or a 1024-bit key.

If the key generation is successful, the message `Command Generate key successful` appears and the system generates the public-private key pair. You can verify that the key pair has been created by using sslcmd option **4** for the **List keys** command.

Step 8 Proceed to the task on the following page.

Creating a Certificate Signing Request

Summary: If you selected a security level of 2 or higher during the PATROL installation procedure, perform the following steps to create a certificate signing request.

Before you can request a certificate from the certificate authority as described below, you must generate a public and private cryptographic key pair (as described in the previous task, "Generating Public and Private Keys for a Certificate" on page 2-20). Next, you assign that key pair to the new certificate for a BMC Software product user or product component. A cryptographic key pair is a set of two cryptographic keys (one publicly shared and one private) used to start an SSL session.

Before You Begin

Complete the steps described in "Generating Public and Private Keys for a Certificate" on page 2-20.

To Create a Certificate Signing Request

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>**(Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **3** for **Generate CSR**.

Step 5 At the **CSR output file name** prompt, enter the file name for the generated CSR.

Step 6 At the **Enter alias name** prompt, enter the alias (identity) name for the key pair that you generated.

The alias is the ID that identifies the public/private key pair. The alias is usually the same as the name of the key database file.

Step 7 When prompted to supply the information of the distinguished name (DN) associated with your new certificate, refer to the table below to help you determine what information is needed for each prompt.

Table 2-6 Distinguished Name Prompts

Prompt	Description of Requested Value
Country	The two-character country code of the certified's resident address. See "Valid Country Codes" on page A-1.
State	The two-character state of the certified's resident address.
Locality	The address of the certified resident.
Name	The organization to which the certified person belongs.
Unit	The body within an organization to which the certified person belongs.
Common name	The name of the entity that you are certifying.
E-mail address	The return e-mail address for the certified person. This value is used by the ESS connection profile ACL_Deny and ACL_Allow configuration variables.

After you complete each of the prompts, a CSR is generated and is ready for you to submit to the trusted CA for signing. If the generation of the signing request is successful, the message `Command Generate CSR successful` appears and the system generates the public-private key pair.

Step 8 Copy and paste the CSR to the vendor site (see "Obtaining a CA Certificate" on page 2-34 and "Installing a Keypair Certificate in the Key Database" on page 2-24).

Step 9 Proceed to the task on the following page.

Installing a Keypair Certificate in the Key Database

Summary: If you selected a security level of 2 or higher during the PATROL installation procedure, perform the following steps to install a certificate in the SSL key database.

Installing a keypair certificate in the SSL key database makes the certificate available to the BMC Software security subsystem for use in secure product communications. You must install the trusted root authority's certificate in the SSL key database before you install a signed certificate in the database.

Before You Begin

- Install the trusted root authority's certificate from the vendor site to the database as described in "Installing a CA Certificate in the Key Database" on page 2-17.
- Generate a CSR and submit it to the vendor site as described in "Creating a Certificate Signing Request" on page 2-22.
- Generate and download the signed certificate from the vendor site.

To Install a Keypair Certificate in the SSL Key Database

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **9** for **Add cert** to add a digital certificate to the SSL key database.

Step 5 At the **Enter certificate file name** prompt, enter the file name for the digital certificate that you downloaded from the vendor site.

The system installs the certificate in the SSL key database.

Note

This completes all required configuration tasks for the SSL key database. The tasks that follow describe optional database management tasks that you can perform using the sslcmd utility.

Listing Public and Private Key Pairs in the Key Database

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 At the prompt, enter the password for the SSL key database file that you want to access.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **4** for **List keys** to list the public/private key pairs in the SSL key database.

For each key pair, the utility displays the label assigned to the certificate that uses the public/private key pair. If no certificate exists, the label has a value of zero and the name of the generated key pair is displayed under the label.

Listing Signed Certificates in the Key Database

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **6** for **List certs** to list the digital certificates installed in the SSL key database.

For each signed certificate, the utility displays the label assigned to the certificate and the information that was assigned using the distinguished name prompts (see Table 2-6, “Distinguished Name Prompts,” on page 2-23).

Viewing Field Information for CA Certificates

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **8** for **View CA**.

Step 5 At the **Enter CA number to view** prompt, enter the number for the CA certificate you wish to view.

Information about the CA certificate in the key database is displayed. After the information is displayed, followed by the confirmation message `Command View CA successful`.

Deleting Trusted Root Authority Certificates

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **10** for **Delete CA**.

Step 5 At the **Enter CA number** prompt, enter the number of the CA certificate that you want to delete. You can obtain the certificate number for a CA from the CA certificate list in the SSL key database by selecting menu option **7** for **List CA**.

The message `Command Delete CA successful` confirms that the certificate has been deleted.

Deleting Private and Public Key Pairs and Certificate

Step 1 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 2 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 3 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 4 At the **Enter a choice** prompt, enter **5** for **Delete keys**.

Step 5 At the **Enter alias name** prompt, enter the alias name of the key pair that you want to delete from the SSL key database.

Step 6 At the **Confirm deletion of** prompt, enter **y** for yes. (Enter **n** if you do not want to delete.)

The message `Command Delete key successful` confirms that the key-pair and associated certificate were successfully deleted from the SSL key database.

Installing a Certificate Revocation List

Step 1 Obtain the new CRL from the trusted CA.

Step 2 At a command line prompt, change to the directory that contains the **sslcmd** utility:

- **%PATROL_HOME%\..\common\security\bin\<*OS*>** (Windows)
- **$PATROL_HOME/../common/security/bin/<*OS*>** (Unix)

Step 3 Enter **sslcmd -k *keyfile.kdb*** to start the **sslcmd** utility.

Step 4 If prompted, enter the password for the key database.

The system displays a menu that contains database commands.

Step 5 At the **Enter a choice** prompt, enter **11** for **Add CRL**.

Step 6 At the **Enter crl file name** prompt, enter the file name of the new CRL that you want to install in the key database.

The named CRL is added to the key database.

Example: Using the sslcmd Utility to Manage the Key Database

This example shows the screens that display and the commands you use to create a key file for level 4 security.

```
sslcmd -K patrol.kdb
-----------------------------------------------------
File new.kdb not found
Enter new key file new.kdb password (8 characters):
Retype password :
-----------------------------------------------------
1. Generate key
2. Add CA
3. Generate CSR
4. List keys
5. Delete key
6. List certs
7. List CA
8. View CA
9. Add Cert
10. Delete CA
11. Add CRL
12. Change password
13. EXIT
Enter a choice [1 - 13]: 1
-----------------------------------------------------
```

STEP 1 - Generate Key - Key alias name must be the same as the user login name

```
Enter alias name:patrol
Enter keypair type, D for DSA, <other> for RSA:
Enter key length 512|1024:512
Command Generate key successful
```

STEP 2 - Generate CSR (Certificate Signing Request)

```
Enter to proceed
-----------------------------------------------------
1. Generate key
2. Add CA
3. Generate CSR
```

```
4. List keys
5. Delete key
6. List certs
7. List CA
8. View CA
9. Add Cert
10. Delete CA
11. Add CRL
12. Change password
13. EXIT
Enter a choice [1 - 13]:  2
-----------------------------------------------------
CSR output file name: output.csr
Enter alias name:patrol
       Country (  2 chars max): US
         State (128 chars max): TX
      Locality (128 chars max): Houston
          Name ( 64 chars max): John Doe
          Unit ( 64 chars max): QA
   Common Name ( 64 chars max): QA
 Email Address (128 chars max): jdoe@bmc.com

Command General CSR successful.
Enter to proceed.
Enter a choice [1 - 13]:  13
```

Copy and paste the CSR to the vendor site.

STEP 3 - Add CA - WWWQA

```
-----------------------------------------------------
1. Generate key
2. Add CA
3. Generate CSR
4. List keys
5. Delete key
6. List certs
7. List CA
8. View CA
9. Add Cert
10. Delete CA
11. Add CRL
12. Change password
```

```
13. EXIT
Enter a choice [1 - 13]:  2
--------------------------------------------------
Enter CA certificate file name.
Command Add CA successful.
Enter to process.
```

STEP 4 - Add Cert in the key file

```
--------------------------------------------------
1. Generate key
2. Add CA
3. Generate CSR
4. List keys
5. Delete key
6. List certs
7. List CA
8. View CA
9. Add Cert
10. Delete CA
11. Add CRL
12. Change password
13. EXIT
Enter a choice [1 - 13]:  9
--------------------------------------------------

Enter certificate file name.
Command Add cert successful
```

Obtaining a CA Certificate

After the user has generated a Certificate Signing Request (CSR) using the utility sslcmd, one may submit the CSR to one of several Certificate Authorities (CA). The CA's response to the CSR is a certificate which may then be loaded into the security module's key database. Once loaded, the certificate may be presented to any peer. This certificate contains a provably genuine copy of the subject's public key.

The certificates that you obtain must be an ASCII text file in version 3 of the X.509 PEM (Privacy-Enhanced Mail) Base64 format. The key database administrator utility (**sslcmd.exe**) uses the X.509 ASCII string format to import certificates. You can obtain these certificates with Microsoft Certificate Server, Netscape Certificate Server, and OpenSSL.

Since the sslcmd utility accepts only those certificates that are base64 encoded, if you have a certificate in format other than Base64, you must obtain and use a translator program to convert the certificate to the X.509 Base64 format. Netscape Certificate Server, and OpenSSL return the certificate in base64 encoding. The Microsoft CA does not. To convert a Microsoft certificate to an X.509 certificate, you would use the Microsoft INETSDK tools

On Microsoft Windows 2000 Server/Advanced Server, you can install the Certificate Service to obtain a CA.

On Microsoft Windows 98 or Windows NT Server 4.0, install Option Pack 4.0 to install the Internet Information Server (IIS) certificate authority/certificate service for CSR Use the **CertUtil.exe** utility that is provided with the IIS installation program and follow the procedure below to generate a base64 encoded version of the Microsoft generated certificate.

Converting a Microsoft CA Certificate to Base64 Format

Step 1 The certificate returned by the Microsoft CA is of file type '.cer'. Save this certificate on a machine running Windows 98 or Windows NT.

Step 2 Double click the certificate's icon.

A Microsoft Certificate Manager dialog box appears.

Step 3 Click the Details tab.

Step 4 Click the **Copy to File** button.

The Certificate Manager Export Wizard appears.

Step 5 Click **Next**.

Step 6 Select **Base64 encoded X.509 (.CER)** and click **Next**.

Step 7 Use the **Browse** button to navigate to the desired save location. Enter a filename using **.cer** as the file type.

Step 8 Click **Save**, then click **Next**.

A message appears stating that the certificate has been successfully exported.

Step 9 Click **Finish**, then click **OK**.

The resulting exported file is now compatible with the sslcmd utility.

PATROL Configuration Files

The following PATROL configuration files contain parameters that pertain to security implementation:

Table 2-7 Configuration Files

Filename	Description
patrol.conf	Contains the Extended Security Interface (ESI) configuration stanza. When you install security (and choose a security level), the system generates a new version of **patrol.conf** and backs up the original version of the file. For more information, see “patrol.conf” on page 2-37.
config.default	The default configuration file for the PATROL Agent. When you install security (and choose a security level), the system generates a new version of **config.default** and backs up the original version of the file. For more information, see “config.default” on page 2-39.
dlls.conf	Lists the .dll files necessary for KMs to work with the PATROL Agent. For more information, see “Configuring the dlls.conf File” on page 2-10.

patrol.conf

The **patrol.conf** file contains the Extended Security Interface (ESI) configuration stanza. (For further information, see “Extended Security Interface (ESI)” on page 2-51.) When you install PATROL and choose a security level, a new version of **patrol.conf** is generated, while the original version of the file is backed up.

The location of the **patrol.conf** file is specified as follows:

- **%PATROL_HOME%\..\common\patrol.d** (Windows)
- **/etc/patrol.d** (Unix)

The following table lists an example of configuration data and a description of each section of data in **patrol.conf**. (Please note the legend at the end of the table.) For more detail on the **patrol.conf** file, see the *PATROL Agent Reference Manual*.

Table 2-8 Configuration Data of patrol.conf (Part 1 of 2)

Stanza and Parameter Name	Level 0 (Basic Security)		Level 1		Level 2		Level 3		Level 4		Description
	C	A	C	A	C	A	C	A	C	A	
[ESI]											ESI stanza name
esi_lib	x	x	x	x	x	x	x	x	x	x	• specifies the path to the PATROL ESI library for the console and agent • install location example is /home/seqqa/PATROL3.3/Solaris25-sun4/bin/bmcesi.so
[AGENT]											agent stanza name
allowsnmpexecute	T	T	T	T	T	T	F	F	F	F	permits or prevents the ability to run PSL commands from an SNMP network monitor
[CONSOLE]											console stanza name
allowcommit	T	T	T	T	T	T	F	F	F	F	permits or prevents the console from committing any KM changes to any connected agents (if you remove this right, PATROL disables menus that provide access to KM commit operations)
allowdeveloper	T	T	T	T	T	T	F	F	F	F	permits or prevents a console from establishing a developer mode connection to an agent

Table 2-8 Configuration Data of patrol.conf (Part 2 of 2)

Stanza and Parameter Name	Level 0 (Basic Security)		Level 1		Level 2		Level 3		Level 4		Description
	C	A	C	A	C	A	C	A	C	A	
allowsysoutputexec	T	T	T	T	T	T	F	F	F	F	permits or prevents a user from entering operating system commands into the PATROL system output window

C = console
A = agent
x = installed
T = true (value)
F = false (value)

config.default

The **config.default** file is the default configuration file for the PATROL Agent. When you install PATROL and choose a security level, a new version of **config.default** is generated, while the original version of the file is backed up.

The location of the **config.default** file is specified as follows:

- **%PATROL_HOME%\lib**(Windows)
- **$PATROL_HOME/lib** (Unix)

The following table describes security-related parameters in the **config.default** file.

Table 2-9 Agent and Console Features in config.default (Part 1 of 2)

Description	Basic Security	Level 1	Level 2	Level 3	Level 4
/AgentSetup/accessControlList					
This variable lists which user names may be used by which consoles when connecting to an agent. The format is a comma-separated list of entries, with each entry being of the form UserName/HostName/Mode. • UserName is the name of a local account that the connecting console may request to use. UserName may be either a single asterisk (*) (meaning that any username is allowed, assuming the account exists), or the actual name of the account. • HostName is the console that is authorized to connect to the agent. HostName may be a single asterisk (*)(meaning that all hosts are allowed to connect), the actual name of a host (indicating that this entry is for that host only), or a wildcard specification, in which the first character is a single asterisk (*) with other characters following. Mode is a list of zero or more of the characters C, D, O, P, and A (see legend). Mode indicates that the host is authorized to connect to the agent in a particular mode and log on as that user.	*/*/CDOPSR	*/*/CDOPSR	*/*/CDOPSR	*/*/COP	*/*/COP
/AgentSetup/PortConnectType					
This variable allows you to select the communication protocols UDP, TCP, or both when binding to a port.	UDP/TCP	UDP/TCP	UDP/TCP	TCP	TCP

Table 2-9 Agent and Console Features in config.default (Part 2 of 2)

Description	Basic Security	Level 1	Level 2	Level 3	Level 4
/AgentSetup/BindToAddress					
This variable allows you to bind the PatrolAgent to a specific network card on a machine with more than one network card.	see [1]	see [1]	see [1]	see [1]	see [1]
/AgentSetup/security/ExtendedSecurityEnabled					
This variable indicates when the ESI is enabled. If this variable is set to "yes," but the ESI library could not be found or loaded, the agent will exit.	yes	yes	yes	yes	yes

[1] The unfilled entries in **config.default** are empty strings.

C = Configure

D = Developer

O = Operator

P = PATROL Event Manager

S = System Output

R = Operator Overwrite

A = Anonymous

TCP = Transmission Control Protocol

UDP = User Datagram Protocol

PATROL Security Policies

To reduce the risk of inadvertent configuration changes or attempted breaches on your computer system, PATROL stores configuration data in a centralized location so that you can apply common administrative rules of protection to your computer environment. Security policies centrally store and manage this data; these security policies define the security behavior of your PATROL installation.

Site Policies and Application Policies

A security policy is defined by entries in one or more configuration files. One such configuration file is referred to as the *site* policy (**site.plc** on Unix; **site** registry on Windows). This default site security policy is the only required policy file; it defines security configuration shared by BMC Software PATROL services. The site policy defines the basic framework of the security policy.

Optionally, you may provide additional files (*application* policies) to supplement the site policy. Application policies contain parameters used by specific applications, such as agents or consoles. For information on which application files pertain to which application, see Table 2-10, “Component Configuration Files,” on page 2-44.

Application policies are useful in situations where a process has more than one context running in the same role. As each context is initialized, the attributes of its security policy are specified initially by the site policy. Selected attributes of the site policy are then modified by the application policy (any attributes specified in the application policy override the attributes of the site policy). Therefore, each context specifies the same site policy but individually specifies a different application policy.

Location of Policy Files and Registry Entries

Separate files store the individual policies: on Unix computers **.plc** files store the policies; on Windows, a **.reg** file sets the registry entries.

On Windows, the policy is set in the following registry entries at **HKEY_LOCAL_MACHINE\Software\BMC Software\Patrol\SecurityPolicy:**

- site
- pcentral
- esi
- agent
- console
- cserver

- signer
- verifier

On Unix, the following policy files are located in **/etc/patrol.d/security_policy:**

- agent.plc
- console.plc
- cserver.plc
- esi.plc
- signer.plc
- site.plc
- verifier.plc

Note

If you uninstall PATROL, you should manually remove these registry entries and policy files.

Component Policy Files

To enable network security between two communicating applications, you are required to create separate client and server policies. Digital signing applications also require separate policies. The types of policies implemented in PATROL include:

- Communication client
- Communication server
- Digital signer
- Digital signature verifier

The following table shows the policy configuration files or Windows registry entries that correspond to each PATROL component. For information on the default mode (attended versus unattended) for each component, see Table 1-2, “Default Modes (Unattended and Attended),” on page 1-12.

Table 2-10 Component Configuration Files

Component	Configuration Files (Unix)	Registry Entries (Windows)
PATROL 3.5 Console	site.plc console.plc	site console
PATROL Central - Microsoft Windows Edition	not applicable	site pcentral
PATROL Agent 3.5	site.plc agent.plc	site agent
PATROL Console Server	site.plc cserver.plc client.plc	site cserver client
PATROL Event Manager 3.5 PATROL 3.4.11 apps (PATROL Classic Console/Agent) PATROL CLI PATROL Link pconfig client apps	site.plc esi.plc	site esi

Note that PATROL version 3.4.11 uses only the site.plc and esi.plc files (on Unix) and the site and esi registry keys (on Windows).

The SignFile utility uses the site and signer policies. The VerifyFile utility uses the site and verifier policies.

Unix Security Policy Implementation

In Unix environments, a security policy is implemented as an ASCII text file. The format of the file is the standard .ini format. The site policy contains stanzas that specify and configure the security module to be loaded in order to support the role defined by that stanza. For example, if an application is going to act as a network server, it adopts the “server” role and its security attributes reside in the [server] stanza. If an application is going to act as a network client, it adopts the “client” role and its security attributes reside in the [client] stanza.

The site policy also contains stanzas defining the signature and verification security policy. The signing and verification policies refer to the keystore and keys that the user creates. If an application is going to sign a file, it adopts the “signer” role and its security attributes reside in the [signer] stanza. If an application is going to verify the signature of a file, it adopts the “verifier” role and its security attributes reside in the [verifier] stanza.

A typical site policy is listed below:

```
[client]
security_level=2
bindir =
/home/pcedergr/ess2.0/bmc/ess/bin/aix_5_000715744c0064
securitydir = /home/pcedergr/ess2.0/bmc/ess/cert
logdir = /tmp
loglevel=ERROR, WARNING, INFO, TRACE

[server]
security_level=2
bindir =
/home/pcedergr/ess2.0/bmc/ess/bin/aix_5_000715744c0064
sksdir = /home/pcedergr/ess2.0/bmc/ess/cert
securitydir = /home/pcedergr/ess2.0/bmc/ess/cert
password=82a153ecffbc901bb73fefe0c23c84b8b76d422a1e6ed
83d,/home/pcedergr/ess2.0/bmc/ess/cert/tree.bin
keyfile=/home/pcedergr/ess2.0/bmc/ess/cert/patrol.kdb
identity = patrol
logdir = /tmp
loglevel=ERROR, WARNING, INFO, TRACE

[verifier]
security_level=3
bindir =
/home/pcedergr/ess2.0/bmc/ess/bin/aix_5_000715744c0064
securitydir = /home/pcedergr/ess2.0/bmc/ess/cert
keyfile=/home/pcedergr/ess2.0/bmc/ess/cert/patrol.kdb
logdir = /tmp
loglevel=ERROR, WARNING, INFO, TRACE

[signer]
security_level=4
```

```
bindir =
/home/pcedergr/ess2.0/bmc/ess/bin/aix_5_000715744c0064
sksdir = /home/pcedergr/ess2.0/bmc/ess/cert
securitydir = /home/pcedergr/ess2.0/bmc/ess/cert
password=82a153ecffbc901bb73fefe0c23c84b8b76d422a1e6ed
83d,/home/pcedergr/ess2.0/bmc/ess/cert/tree.bin
keyfile=/home/pcedergr/ess2.0/bmc/ess/cert/patrol.kdb
identity = bmc_signer
logdir = /tmp
loglevel=ERROR, WARNING, INFO, TRACE
```

Windows Security Policy Implementation

A security policy is defined by string entries made into one or more registry keys placed in the Windows registry. One registry key, which is required, defines the site policy. Its path in the registry is

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Bmc Software\
patrol\SecurityPolicy\site
```

You may provide additional keys at the security policy level to supplement the site policy. These keys each implement an application policy. The basic framework of the security policy is defined in the site policy. Application polices define additional details, if needed. For information on the location of the application policies, see “Component Policy Files” on page 2-43.

The site policy contains keys that specify and configure the security module to be loaded in order to support the function defined by the stanza. The role that the application is playing (client or server) defines the communications security policy. Thus, the site policy contains the following two communication registry keys:

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\
Bmc Software\patrol\SecurityPolicy\site\client
```

and

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\
Bmc Software\patrol\SecurityPolicy\site\server
```

The site policy also contains keys defining the signature and verification security policy. If an application is going to sign a file, its configuration resides in

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Bmc Software\
patrol\SecurityPolicy\site\signer
```

If an application is going to verify the signature of a file, its configuration resides in

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Bmc Software\
patrol\SecurityPolicy\site\verifier
```

The typical layout of a site policy for Windows servers is similar to the layout shown in “Unix Security Policy Implementation” above.

Policy Attributes

Each policy may contain the following name/values pairs. Each stanza (or key) may contain some or none of these attributes. No stanza (or key) requires all the attributes to be present, since some attributes do not apply in certain roles and some do not apply at certain security levels. Other attributes are fixed in certain contexts and cannot be changed by the configuration. For information about error messages related to missing or invalid entries in these fields, see “Troubleshooting” on page 3-5. Ensure that all file path conventions comply with OS naming conventions.

- **Security_level = level** specifies the network provider module and protocol used at runtime. The value will equal one of the security levels **0** (basic, default security level) through **4**.

Note

If the **security_level** field is deleted or contains an empty string, the level of security defaults to **4**. Note that this differs from the PATROL installation process, which defaults to **0** (basic security level).

- **Bindir = binpath** specifies the directory of the security 32 bits library.

- **Bindir64 = bin64path** specifies the directory of the security 64 bits library.

- **Sksdir** is not currently used.

- **Securitydir = secpath** specifies the directory where sensitive key information is stored (for example, SSL keystore or key material files).

- **Password = encrypted_password, keymaterialfile location, [optional lock mode]** specifies an encrypted password for unattended service, key material file, and an optional lock mode required to retrieve the master password for the SSL keystore and SKS databases. The password keyword is used to supply an unattended service start-up password; only the SERVER type of policy or application reads this password keyword.

  The **encrypted _password** field is the encrypted password generated by the offline password encoding program. For more information, see “Using the plc_password Utility” on page 3-3. The password encryption method is based on Triple DES PCBC cipher and CBC checksum. The Triple DES encryption keys and IV data are derived from user supplied key material file. To prevent “password stealing,” password encryption can be optionally locked by user name or IP address.

  The **keymaterialfile** field is the file that you supply and protect, that is used for 3 DES key computation.In an operational environment, you should limit file exposure to the service start-up only, and physically remove a file (for example, from a floppy disk drive) once the service is running. The user is responsible for the protection and security risk taken due to the selection of an unattended service startup. For a discussion of the security risks inherent in unattended operation, see the “Unattended and Attended Modes” section.

The **lock_mode field - user** or **ip**- specifies additional data inserted using a 3 DES key for password encryption. When **user** lock mode is specified, the user name (not the user account of the machine) is inserted into the computation of an encryption key. To decrypt an encrypted password, an application uses its owner/userid in key computation.

When **ip** lock mode is specified, an IP address of a specified host will be inserted into key computation. The encrypted password can be decoded only on a machine with the same IP address as when the password was encrypted or decrypted. For more information, see "Using the plc_password Utility" on page 3-3.

- **keyfile = keyfile_path** specifies the location of a PKI/SSL keystore database.

- **Identity = keyname** specifies the name or label where the signing key is stored in the PKI/SSL keystore. The digital signature verification policy requires only the keyfile entry, since the verification process does not use an identity.

- **logdir = logdir** specifies the absolute path to a subdirectory where the log file will be written.

- **logfile = logfile** specifies the log file path. When only a file name is provided, the log file is created in the current working directory.

- **loglevel = ERROR, WARNING, INFO, TRACE** specifies log level desired. Any comma-separated combination of ERROR, WARNING, INFO, or TRACE tokens can be used to generate error, warning or diagnostics log messages. In order to get the security level information, you must include the INFO field.

Working with Configuration Files

This section describes tasks that you may need to perform in the configuration files and policy files/registry keys described in the previous sections.

Using PATROL Event Manager Applications with PATROL Security

When using PATROL Security at levels 1 through 4, the PATROL Event Manager (PEM) applications need to be recompiled with the PEM library only if with the applications are to be compatible with the 3.5 PEM APIs.

To configure PATROL Security, perform the following steps.

Step 1 Configure the following parameter in the **config.default** file as shown:

```
"/AgentSetup/security/ExtendedSecurityEnabled" = {
REPLACE="yes"}
```

Step 2 Configure the following parameter in the **patrol.conf** file as shown:

```
esi_lib = <location of the esi library >
```

Step 3 On Windows, set the registry HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\PATROL\ as shown:

```
PATROL Agent = <the esi_lib path location>

PATROL Security = <directory where patrol.conf is
located>
```

At security level 4, the PEM client application may be launched by a system user rather than a login user. In this case, a certificate with `identity = system` must exist in the client key database for the authentication with the server application (for example, the PATROL Agent). If the application is launched by a login user rather than a system, then use `identity = username`.

Using attended mode on Windows, where the user is required to enter a password for the keyfile to get certificate information, the PEM service needs to be able to interact with Desktop. Refer to “Unattended and Attended Modes” on page 1-11.

Configuring the Access File

For server policies running security level 4, an **access** file is located in **%PATROL_HOME%\..\common\security\keys** (Windows) or **$PATROL_HOME/../common/security/keys** (Unix) and contains the following default values:

```
[SSL_SERVER]

ALLOW_ACL = *

DENY_ACL =
```

This setting allows all authorized by default to access the server; none are denied. You can specifically deny access by inserting the email address DN into the DENY_ACL attribute, as shown in the following example. (See “Distinguished Name Prompts” on page 2-23.)

```
ALLOW_ACL = *

DENY_ACL = johnsmith@abc.com
```

In the example above, all authorized users would be allowed access to the server except for the user with email address johnsmith@bmc.com.

Extended Security Interface (ESI)

The ESI pluggable security component allows you to specify the PATROL security plug-in used to ensure privacy of communications between PATROL components. For more information about the ESI pluggable security component, see the *PATROL Agent Reference Manual*.

ESI in PATROL 3.5

In the **patrol.conf** file, the esi_lib32 and esi_lib64 variables specify the ESI library location for 32 bit or 64 bit installed products, respectively. Table 2-11 describes these variables.

Table 2-11 Group Definition Types and Variables

Variables	Valid Values	Description
`esi_lib32`	the path of the 32-bit ESI library or **none** if no ESI library is being used The default value for the `esi_lib32` variable is **none**.	specifies a 32-bit ESI library to use for authentication and encryption
`esi_lib64`	the path of the ESI library or **none** if no ESI library is being used The default value for the `esi_lib64` variable is **none**.	specifies a 64-bit ESI library to use for authentication and encryption

The ESI variables appear in the **patrol.conf** file as follows:

Unix:

```
#[ESI]

esi_lib =
$PATROL_HOME/common/security/bin/<OS>/bmcesi.so

esi_lib32=
$PATROL_HOME/common/security/bin/<OS>/bmcesi.so

esi_lib64=
$PATROL_HOME/common/security/bin/<OS>/bmcesi.so
```

Windows:

```
#[ESI]

esi_lib =
%PATROL_HOME%\common\security\bin\<OS>\bmcesi.dll
```

```
esi_lib32=
%PATROL_HOME%\common\security\bin\<OS>\bmcesi.dll

esi_lib64=
%PATROL_HOME%\common\security\bin\<OS>\bmcesi.dll
```

On Unix, the following fields resides in the [client], [server], [signer], and [verifier] sections of the site policy file (**site.plc**).

bindir = **binpath**, specifies the directory of the security 32 bits library.

bindir64 = **bin64path**, specifies the directory of the security 64 bits library.

For more information about using an ESI library, see the *PATROL API Reference Manual*.

ESI in PATROL 3.4

There are certain differences in the behavior between security-enabled PATROL 3.4 and security-enabled PATROL 3.5.

In PATROL 3.4, the application component does not load the application policy, therefore the default for all components is always site.plc and esi.plc (Unix) or the site and esi registry keys (Windows). Consequently, all logs from PATROL Console, pconfig, PatrolCLi...etc will go to the same log. This behavior differs from PATROL 3.5, in which the application policy is loaded for each application component.

In addition, PATROL 3.4 for Unix does not support the esi_lib32 and esi_lib64 variables described in Table 2-11, “Group Definition Types and Variables,” on page 2-52. Instead, the esi_lib variable is used by default; the distinction between 32 bit and 64 bit applications must be manually adjusted by modifying esi_lib in the patrol.conf file. Modify the file for the applicable platform as shown in the table below.

Table 2-12 Configuration of patrol.conf

Platform	PATROL CONSOLE (GUI apps, emcons, xpconfig, PatrolLink) Uses 32 bits library for 32 bits PEM Application	PATROL AGENT (Commandline apps, pconfig, PatrolCli) Uses 64 bits library for 64 bits PEM Application
Reliant 5.45/5.44 64 bits	/etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/reliant-5-44-r10000 /bmcesi.so	/etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/reliant-5-44-r1000064/bmcesi.so
AIX 4.3 64 bits	/etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/aix-4-3-rs/bmcesi.so	/etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/aix-4-3-rs-64/bmcesi.so
HP 11 64bits	/etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/hpux-10-20-pa11/bmcesi.so	/etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/hpux-11-11-pa20-64/bmcesi.so or /etc/patrol.conf esi_lib = <INSTALL_DIR>/common/security/bin/hpux-11-00-pa20-64/bmcesi.so

Note

In PATROL 3.4, the correct syntax for the esi_lib variable requires a space before and after the “=” symbol.

Using PATROL Security Tools

This chapter describes the various PATROL security configuration utility tools available, including procedures you can perform to customize your security environment using the SSL protocol. The following topics are discussed in this chapter:

PATROL Security Utilities

When you install PATROL, the following security tools and utilities are installed:

Table 3-1 PATROL Security Utilities

Name	Description	For instructions, see...
sslcmd	use to manage the key database	"Key Database Management" on page 2-12
plc_password	allows you to switch between attended and unattended modes and to change the key database password	"Setting Unattended Mode and Password Encryption" on page 3-2
signFile	used to sign the file used in the site policy	"Digital Signing" on page 3-4
verifyFile	verifies the signed file	"Digital Signing" on page 3-4
esstool	a diagnostic tool that provides information on security level and configuration	"Troubleshooting" on page 3-5

Setting Unattended Mode and Password Encryption

The plc_password utility, located in **%BMC_ROOT\..\common\security\bin\<*OS*>** (Windows) or **$BMC_ROOT/../common/security/bin/<*OS*>** (Unix), is the command-line utility you use to switch between attended and unattended modes and to change the password on your key database file.

This tool allows you to create, update, or remove the security policy's unattended operation password field. You can also use plc_password to to change the key database password.

The plc_password tool prompts for the new master password, encrypts the master password using the user-supplied key material file, and stores the master password in the password field. To satisfy US export law, the master password/passphrase length is limited to 64 characters.

For more information on the differences between attended and unattended modes, and the security risks inherent in using unattended mode, see Table , “Unattended and Attended Modes,” on page 1-11.

Note

On Unix, you must be logged in as root in order to change your password using plc_password.

Using the plc_password Utility

The following describes correct usage syntax for the plc_password tool:

```
plc_password
-r <client>|<server>|<signer>|<verifier> --- Role ,
specifies security policy role to update
-P <policy>, specifies policy path, i.e.
/etc/patrol.d/security_policy/agent.plc or
Patrol\SecurityPolicy\agent key on NT.
-m <attended>|<unattended> --- make
attended/unattended operation mode, either removes or
creates the policy password field.
[ -v ] --- print version and exit
[ -h ] --- print usage and exit
      ---unattended mode parameters---
  -f <key material file>  , a user owned file on data
used for password protection, the file should be at
least 1024 bytes long.
 [-H <hostname>] --- lock by ip address, creates
password entry readable on the <hostname> machine only
  [-u <username>] --- lock by username, creates
password entry  readable by a process owned by a user
  [-c ]           --- change key database password,
applies newly entered master password to the PKI
keyfile
  [-k <key database file>, PKI keyfile  contains
public-private keys, X509 user and Trusted Roots
Certificates.
```

Digital Signing

The signFile and verifyFile utilities are used to sign and verify the files used in the site policy.

Using the signFile Utility

Use the signFile utility, located in **%BMC_ROOT\..\common\security\bin\<*OS*>** (Windows) or **$BMC_ROOT/../common/security/bin/<*OS*>** (Unix), to sign the file used in the specified policy. The SignFile utility appends a filename with the **.sgn** extension and stores the ***file*.sgn** file in the directory specified by -s option. In the absence of -s option, stores file.sgn in the same directory where the original file resides.

The following describes correct usage syntax for the signFile utility:

```
signFile
file -[s signature_subdirectory] -[v]  [-V] [-h] [-v]
[-]
file - file to sign
-s   - signature directory
-S   - Site Policy
-P   - Application/Signer policy
-v   - print version
-V   - verbose
-h   - helpwhere
```

Using the verifyFile Utility

Use the verifyFile utility, located in **%BMC_ROOT\..\common\security\bin\<*OS*>** (Windows) or **$BMC_ROOT/../common/security/bin/<*OS*>** (Unix), to verify that a file has been properly signed using the trusted root key file with the certificate. The utility checks for a ***file*.sgn** file in the **signer** attribute and returns a confirmation if signed, or an error message if no ***file*.sgn** exists.

See “Using the signFile Utility” on page 3-4 for information on signing a file.

The following describes correct usage syntax for the verifyFile utility:

```
verifyFile
file [-s signature directory] -[v]  [-V] [-h] [-v] [-S
s]
file - file to sign
-s   - signature directory
-S   - Site Policy
-P   - Application/Signer policy
-v   - print version
-V   - verbose
-h   - help
```

Troubleshooting

This section provides troubleshooting information regarding PATROL Security components.

Log Files

When encountering security-related errors, including configuration errors, consult the log files. The log files are located in **%BMC_ROOT%\..\common\security\log** (Windows) or **$BMC_ROOT/../common/security/log** (Unix).

These log files contain error, warning, and trace information on security communication as well as the security levels designated for each component. The **logdir** and **logfile** attributes of the site policy and application policy specify the name and location of the log file for each policy.

Using the esstool Utility

The esstool utility is located in**%BMC_ROOT\..\common\security\bin\<*OS*>** (Windows) or **$BMC_ROOT/../common/security/bin/<*OS*>** (Unix). The esstool utility is a diagnostic tool that provides information about the security configuration, communication authentication, password encryption, version information, and security module capabilities.

The following describes correct usage syntax for the various esstool functions:

Security Diagnostics Tool

```
esstool
-v,             version
query,          network security module (SSL, DH)
capabilities
policy,         security policy content
server,         TCP/IP sample server
client,         TCP/IP sample client
bpwm,           password encryption
auth,           authentication
```

Security Policy Content

```
esstool policy
-r <str>  - role (client,server,signer or verifier)
  -a        - long dump of security policy
  -b        - security bootstrap/initialization
  -S <path> - site policy
  -P <path> - application policy
  -?        - help
```

Security Module Capabilities

You can use esstool to view information about a security module. In the example usage the follows, information is returned regarding the version, type of authentication, and ciphers that the bmcsslDomestic module is using.

Example (Unix):

```
esstool query ./bmcsslDomestic.so
doing BMC_LoadModule ./bmcsslDomestic.so
Module ./bmcsslDomestic.so loaded

Security Module capabilities (./bmcsslDomestic.so)
---------------------------------------------------

version:        SSL Module, Version
1.0|ess2.0.d.5.6|sunos_5.5.1_sun4u|Jan 23
2002|20:28:30


(Domestic)
authentication: MUTUAL
ciphers v2:     rsa_with_rc4_128_sha,
rsa_with_rc4_128_md5, rsa_with_des_cbc_sha, ...(list
of ciphers appears)
authorization:  SERVER_ACL
```

Secure Channel TCP/IP Server

```
esstool server
Valid options:
  -h <str>  - hostname
  -p <num>  - port
  -s <str>  - service name
  -L <num>  - security level
  -S <path> - site policy
  -P <path> - application policy
  -V <str>  - module's version
  -n        - nonblocking io
  -?        - help
```

Secure Channel TCP/IP Client

```
esstool client
Valid options:
  -h <str>  - hostname
  -p <num>  - port
  -s <num>  - sleep time (sec)
  -L <num>  - security level
  -S <path> - site policy
  -P <path> - application policy
  -V <str>  - module's version
```

```
  -r <str>  - HTTP request
  -u <str>  - user identity
  -k <str>  - keyfile path
  -n        - nonblocking i/o
  -?        - help
```

Password Encipherment

```
esstool bpwm
-m <str> - encryption shared library path (required) -
.../bmk
  -c <str> - cipher name (default:des-cbc)
  -p <str> - password string (required)
  -l <str> - lock string used to perturb password
(optional)
  -e <str> - string to encrypt (-e OR -d required)
  -d <str> - string to decrypt (-e OR -d required)
  -D       - decrypt the results of encryption
(requires -e opt)
  -n <num> - number of time to repeat (default = 1)
  -?        - help
```

Authentication Tester

```
esstool auth
-d <str> - NT domain to authenticate against (default
is null)
  -u <str> - username string (required)
  -p <str> - password string (required)
  -n <num> - number of time to repeat (default = 1)
  -w       - use shadow password
  -S <path> - site policy
  -P <path> - application policy
  -l        - preload auth module via policy LoadMask
  -?        - help
```

Issues and Workarounds

This section identifies errors that you may encounter when working with PATROL security components, identifies the corresponding causes, and provides diagnostic solutions, if applicable.

Issue: The stty terminal settings can affect the operation of the **sslcmd** command. For terminal setting **stty -a**, the following error may appear when choosing **sslcmd** command option **2** (Generate CSR):

The **@** character in the email address field may be read as a "kill" character, such that the email address is truncated.

Cause: Terminal setting **stty -a** is not supported. Enter an alternative terminal setting, such as **stty kill^U**.

Issue: On some platforms, extended error messages may appear when choosing **sslcmd** command option **1** (Generate Key).

Examples

On HP 11.0 (64 bit):

```
/usr/bin/ps: illegal option -- c
usage: /usr/bin/ps [-edaflP] [-u ulist] [-g glist] [-p
plist] [-t tlist] [-R prmgroup]
Command Generate key successful
Enter to proceed
```

On Dynix:

```
Unable to add to port table: "snmp 161/udp"
Possible duplicate entry in services file
Command Generate key successful
Enter to proceed
```

After the error messages appear the key is generated successfully; therefore, no action is required.

Cause: The code generates a stream of unpredictable bytes by performing a list of system calls to selected utilities, for example, ps, netstat, and vmstat. If a certain platform does not to support one or more of the utilities, an error message may appear.

Because the command successfully generates the key, no user action is required and the error message can be ignored.

Issue: The security policy level defaults to level 4 unexpectedly.

Cause: In the site policy file, if the **security_level** field is deleted or contains an empty string, the default level of security is set to 4. Note that this differs from the default 0 (basic security level) that is set during PATROL installation if no security level is specified.

Solution: Specify the desired security policy level in the **security_level** field.

Issue: An error message appears in the log file stating that there is a missing bindir.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **bindir** field was deleted.

Solution: Include the **bindir** field in the file.

Issue: An error message appears in the log file stating that there is a missing securitydir.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **securitydir** field was deleted.

Solution: Include the **securitydir** field in the file.

Issue: An error message appears in the log file stating that there is a missing **sksdir**.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **sksdir** field was deleted.

Solution: Include the **sksdir** field in the file.

Issue: An error message appears in the log file stating that the password prompter was cancelled.

Cause: The user cancelled the password dialog box.

Issue: An error message appears in the log file stating that the password entry requires 2 fields (**password** and **keymaterial**) followed by an optional lock string.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **password** field requires an entry for both a password and key material file, which may have been deleted in order to run in attended mode.

Solution: Include a valid entry in the **password** field.

Issue: An error message appears in the log file stating that the key file cannot be reached.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **keyfile** field may contain an invalid entry or may reference an invalid directory.

Solution: Include a valid entry in the **keyfile** field.

Issue: An error message appears in the log file stating that there was an error decrypting the stored password.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **password** field may contain an invalid password.

Solution: Include a valid entry in the **password** field.

Issue: An error message appears in the log file stating that the identity does not appear in the key database.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **identity:** field may contain an invalid entry.

Solution: Include a valid entry in the **identity** field.

Issue: A password prompt unexpectedly appears.

Cause: In the site file (**site.plc** on Unix, **site.reg** on Windows), the **password** field have been deleted, or the keyfile or password entry in this field may have been deleted. This can occur when a user wishes to run in attended mode, and thus intentionally deletes the password field in order to enable the password prompt to appear.

Solution: To revert to unattended mode, include valid entries in the **password** field.

Issue: Installation of PATROL Security fails.

Cause: Installation may fail due to lack of privilege. On Unix, you may lack the privilege for modifying the **/etc** directory; therefore you cannot create the **/etc/patrol.d/security_policy** or place the policy files in **/etc/patrol.d**.

On Windows, you may lack administrator privilege to modify registry entries; therefore you cannot create the necessary registry entries.

Solution: Obtain an account with the requisite privilege.

Issue: Uninstall fails to remove the security registry entries (Windows) or policy files (Unix).

Solution: Manually remove the security registry entries and policy files.

Issue: The key database will not open although you entered the correct password.

Cause: A 32-bit platform cannot use a key database generated on a 64-bit platform.

Cause: In an international context, a key database generated in one locale cannot be opened in another locale.

Issue: The key database will not open although you entered the correct password.

Cause: A 32-bit platform cannot use a key database generated on a 64-bit platform.

Cause: In an international context, a key database generated in one locale cannot be opened in another locale.

Issue: An SSL server or client opens the key database, but refuses an SSL connection due to a “no key for negotiated cipher” error.

Cause: The key associated with the SSLIdentity was found in the key database, but a certificate guaranteeing its authenticity was not found.

Cause: The SSLV2CipherSuite or the SSLV3CipherSuite attribute limits the list of possible cipher suites that can be used by the server or client. A common cipher suite supported by both cannot be found.

Issue: This certificate cannot be installed into the key database.

Cause: This certificate does not pertain to any key pair contained in the key database.

Cause: The CA certificate used to sign this certificate has not been previously installed in the key database.

Cause: A CA certificate has been installed in the key database, but it is not the CA certificate used to sign this certificate.

Cause: This certificate has (mistakenly) previously been installed in the key database as a CA certificate.

Issue: A certificate revocation list (CRL) cannot be installed into the key database.

Cause: The CA certificate of the CA to which this CRL pertains has not been previously installed into the key database.

Issue: A Windows Certificate Authority rejects a certificate signing request (CSR) which contains the public key of a DSA key pair.

Cause: The Windows Certificate Authority will not generate a certificate for a DSA key pair.

Issue: The default ASCII Password Dialog prompts for the keyfile and password selection on operating systems s390/Linux and Siemens Sinix 5.43, or for systems where the X11 runtime environment is not configured. Using the keyboard-based ASCII prompt is possible only by a foreground process.

Solution: For non-GUI configuration requiring an attended password entry, the PatrolAgent service must run directly from a user shell. The PatrolAgent script should not be used. Run PatrolAgent from the PATROL3/<OS>/bin directory.

Issue: The password prompt fails to display when starting the agent or console for Unix.

Solution: Specify your machine as the hostname:

```
$ DISPLAY=<hostname>:0.0
```

Issue: When using the scripts file in PATROL3 to start the PATROL Console and Agent on Unix in attended mode (password required), the password dialog does not receive standard input.

Solution: Perform one of the following:

- If you wish to run in attended mode, start the PATROL Console and Agent from the **PATROL3/<*OS*>/bin** directory. Be aware that starting the console and agent from the bin directory prevents the Perform Agent, dcm, and bgscollect services from running.

- If you wish to run the Perform Agent, dcm, and bgscollect services, you can start the PATROL Console and Agent from the **PATROL3** directory, but you must run in unattended mode.

Issue: When running PEM-based services, including the console, agent, and any other PEM-based applications, as a service under the domain account, the Password Dialog prompt does not appear.

Solution: Perform one of the following:

- If you wish to use attended mode, run the PEM-based service at the command line under the local system account or run it as a service using the system account and allowing the service to interact with the desktop.
- If you wish to run the PEM-based service as a service under the domain account, use unattended mode.

Issue: The PATROL KM for Microsoft Cluster Server does not operate in attended mode with Level 4 security.

Solution: Attended mode does not support the use of services running under a domain account. Since the Cluster Service runs only under a domain account, you are unable to run this service in attended mode.

Issue: PATROL fails to discover the shared library API km.

Solution: For security levels 1 through 4, all dll files must have signature files (api.dll.sgn) in order to load. To create signature files, use the signFile utility located in %BMC_ROOT/common/security/bin/<target> (Unix) or %BMC_ROOT\common\security\bin\<target> (Windows).

Once you have created signature files for the dll files, perform either of the following:

- In the **patrol.conf** file, in the `'agentrights'` section under the `[AGENT]` stanza, change the `allowalldlls` attribute to `allowalldlls=true`.

- In **/etc/patrol.d/dlls.conf**, list all DLL file(s) and directories that the agent is authorized to load. A template file for **dlls.conf** is loaded during installation and resides in **/etc/patrol.d**.

Issue: Discovery does a ping for UDP. If you selected only the TCP network connection option during installation, discovery fails.

Solution: In the config.default file, comment out the following line:

```
"/AgentSetup/PortConnectType"= {REPLACE="TCP"}
```

Issue: When entering a newly created .kdb file and password in the Password Dialog box, the system fails to validate the correct password for 64-bit key files and an “Incorrect password” message appears.

Cause: A key database created by a 64-bit sslcmd application cannot be opened by a 32-bit application. Similarly, a key database created by a 32-bit sslcmd application but opened and subsequently modified by a 64-bit sslcmd application can no longer be opened by the 32-bit application. In short, key databases are, in general, not transportable between 32-bit and 64-bit platforms.

Issue: When running PATROL Console Server (or any service which must run in attended mode at level 4) as a service under the domain account, the Password Dialog prompt does not appear.

Solution: Perform one of the following:

- If you wish to use attended mode, run Console Server at the command line under the local system account or run it as a service using the system account and allowing the service to interact with the desktop.

- If you wish to run Console Server as a service under the domain account, use unattended mode.

Appendix A

This appendix provides valid country codes for the Distinguished Name prompt “Country” as used by the sslcmd utility. For more information, see “Distinguished Name Prompts” on page 2-23 and “Using the sslcmd Utility” on page 2-12.

Valid Country Codes

The table below contains the valid two-letter ISO codes for the following countries.

Table A-1 Valid Country Codes

COUNTRY	CODE
AFGHANISTAN	AF
ALBANIA	AL
ALGERIA	DZ
AMERICAN SAMOA	AS
ANDORRA	AD
ANGOLA	AO
ANGUILLA	AI
ANTARCTICA	AQ
ANTIGUA AND BARBUDA	AG

Table A-1 Valid Country Codes

COUNTRY	CODE
ARGENTINA	AR
ARMENIA	AM
ARUBA	AW
AUSTRALIA	AU
AUSTRIA	AT
AZERBAIJAN	AZ
BAHAMAS	BS
BAHRAIN	BH
BANGLADESH	BD
BARBADOS	BB
BELGIUM	BE
BELIZE	BZ
BENIN	BJ
BERMUDA	BM
BHUTAN	BT
BOLIVIA	BO
BOSNIA HERCEGOVINA	BA
BOTSWANA	BW
BOUVET ISLAND	BV
BRAZIL	BR
BRITISH INDIAN OCEAN TERRITORY	IO
BRUNEI DARUSSALAM	BN
BULGARIA	BG
BURKINA FASO	BF
BURUNDI	BI
BELARUS	BY
CAMBODIA	KH

Table A-1 Valid Country Codes

COUNTRY	CODE
CAMEROON	CM
CANADA	CA
CAPE VERDE	CV
CAYMAN ISLANDS	KY
CENTRAL AFRICAN REPUBLIC	CF
CHAD	TD
CHILE	CL
CHINA	CN
CHRISTMAS ISLAND	CX
COCOS (KEELING) ISLANDS	CC
COLOMBIA	CO
COMOROS	KM
CONGO	CG
COOK ISLANDS	CK
COSTA RICA	CR
COTE D'IVOIRE	CI
CROATIA	HR
CUBA	CU
CYPRUS	CY
CZECH REPUBLIC	CZ
CZECHOSLOVAKIA	CS
DENMARK	DK
DJIBOUTI	DJ
DOMINICA	DM
DOMINICAN REPUBLIC	DO
EAST TIMOR	TP
ECUADOR	EC

Table A-1 Valid Country Codes

COUNTRY	CODE
EGYPT	EG
EL SALVADOR	SV
EQUATORIAL GUINEA	GQ
ESTONIA	EE
ETHIOPIA	ET
FALKLAND ISLANDS (MALVINAS)	FK
FAROE ISLANDS	FO
FIJI	FJ
FINLAND	FI
FRANCE	FR
FRENCH GUIANA	GF
FRENCH POLYNESIA	PF
FRENCH SOUTHERN TERRITORIES	TF
GABON	GA
GAMBIA	GM
GEORGIA	GE
GERMANY	DE
GHANA	GH
GIBRALTAR	GI
GREECE	GR
GREENLAND	GL
GRENADA	GD
GUADELOUPE	GP
GUAM	GU
GUATEMALA	GT
GUINEA	GN
GUINEA-BISSAU	GW

Table A-1 Valid Country Codes

COUNTRY	CODE
GUYANA	GY
HAITI	HT
HEARD AND MC DONALD ISLANDS	HM
HONDURAS	HN
HONG KONG	HK
HUNGARY	HU
ICELAND	IS
INDIA	IN
INDONESIA	ID
IRAN (ISLAMIC REPUBLIC OF)	IR
IRAQ	IQ
IRELAND	IE
ISRAEL	IL
ITALY	IT
JAMAICA	JM
JAPAN	JP
JORDAN	JO
KAZAKHSTAN	KZ
KENYA	KE
KIRIBATI	KI
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	KP
KOREA, REPUBLIC OF	KR
KUWAIT	KW
KYRGYZSTAN	KG
LAO PEOPLE'S DEMOCRATIC REPUBLIC	LA

Table A-1 Valid Country Codes

COUNTRY	CODE
LATVIA	LV
LEBANON	LB
LESOTHO	LS
LIBERIA	LR
LIBYAN ARAB JAMAHIRIYA	LY
LIECHTENSTEIN	LI
LITHUANIA	LT
LUXEMBOURG	LU
MACAU	MO
MADAGASCAR	MG
MALAWI	MW
MALAYSIA	MY
MALDIVES	MV
MALI	ML
MALTA	MT
MARSHALL ISLANDS	MH
MARTINIQUE	MQ
MAURITANIA	MR
MAURITIUS	MU
MEXICO	MX
MICRONESIA	FM
MOLDOVA, REPUBLIC OF	MD
MONACO	MC
MONGOLIA	MN
MONTSERRAT	MS
MOROCCO	MA
MOZAMBIQUE	MZ

Table A-1 Valid Country Codes

COUNTRY	CODE
MYANMAR	MM
NAMIBIA	NA
NAURU	NR
NEPAL	NP
NETHERLANDS	NL
NETHERLANDS ANTILLES	AN
NEUTRAL ZONE	NT
NEW CALEDONIA	NC
NEW ZEALAND	NZ
NICARAGUA	NI
NIGER	NE
NIGERIA	NG
NIUE	NU
NORFOLK ISLAND	NF
NORTHERN MARIANA ISLANDS	MP
NORWAY	NO
OMAN	OM
PAKISTAN	PK
PALAU	PW
PANAMA	PA
PAPUA NEW GUINEA	PG
PARAGUAY	PY
PERU	PE
PHILIPPINES	PH
PITCAIRN	PN
POLAND	PL
PORTUGAL	PT

Table A-1 Valid Country Codes

COUNTRY	CODE
PUERTO RICO	PR
QATAR	QA
REUNION	RE
ROMANIA	RO
RUSSIAN FEDERATION	RU
RWANDA	RW
ST. HELENA	SH
SAINT KITTS AND NEVIS	KN
SAINT LUCIA	LC
ST. PIERRE AND MIQUELON	PM
SAINT VINCENT AND THE GRENADINES	VC
SAMOA	WS
SAN MARINO	SM
SAO TOME AND PRINCIPE	ST
SAUDI ARABIA	SA
SENEGAL	SN
SEYCHELLES	SC
SIERRA LEONE	SL
SINGAPORE	SG
SLOVAKIA	SK
SLOVENIA	SI
SOLOMON ISLANDS	SB
SOMALIA	SO
SOUTH AFRICA	ZA
SPAIN	ES

Table A-1 Valid Country Codes

COUNTRY	CODE
SRI LANKA	LK
SUDAN	SD
SURINAME	SR
SVALBARD AND JAN MAYEN ISLANDS	SJ
SWAZILAND	SZ
SWEDEN	SE
SWITZERLAND	CH
SYRIAN ARAB REPUBLIC	SY
TAIWAN, PROVINCE OF CHINA	TW
TAJIKISTAN	TJ
TANZANIA, UNITED REPUBLIC OF	TZ
THAILAND	TH
TOGO	TG
TOKELAU	TK
TONGA	TO
TRINIDAD AND TOBAGO	TT
TUNISIA	TN
TURKEY	TR
TURKMENISTAN	TM
TURKS AND CAICOS ISLANDS	TC
TUVALU	TV
UGANDA	UG
UKRAINE	UA
UNITED ARAB EMIRATES	AE

Table A-1 Valid Country Codes

COUNTRY	CODE
UNITED KINGDOM	GB
UNITED STATES	US
UNITED STATES MINOR OUTLYING ISLANDS	UM
URUGUAY	UY
USSR	SU
UZBEKISTAN	UZ
VANUATU	VU
VATICAN CITY STATE (HOLY SEE)	VA
VENEZUELA	VE
VIET NAM	VN
VIRGIN ISLANDS (BRITISH)	VG
VIRGIN ISLANDS (U.S.)	VI
WALLIS AND FUTUNA ISLANDS	WF
WESTERN SAHARA	EH
YEMEN, REPUBLIC OF	YE
YUGOSLAVIA	YU
ZAIRE	ZR
ZAMBIA	ZM
ZIMBABWE	ZW

Glossary

access control list	A list that is set up by using a PATROL Agent configuration variable and that restricts PATROL Console access to a PATROL Agent. A PATROL Console can be assigned access rights to perform console, agent configuration, or event manager activities. The console server uses access control lists to restrict access to objects in the COS namespace.
authentication	A method of proving a person's identity.
certificate	A digital document containing a public key and a name used to authenticate the identity of the source of the data accompanying the certificate. Provides binding between private key and a user.
console server	A server through which PATROL Central and PATROL Web Central communicate with managed systems. A console server handles requests, events, data, communications, views, customizations, and security.
Diffie-Hellman public key	A public key algorithm that allows participants to generate public-private keys, exchange public and private keys, and commute a common session key.
digital signature	Digitally signed hash of a user data.
distinguished name (DN)	The fully-qualified hierarchical names that uniquely identify a specific entity that is authenticated by a digital certificate.

encryption key

A key that is used by an encryption algorithm to encrypt a message or data.

Extended Security Interface (ESI)

A PATROL API that provides vendor-independent security enhancements such as user authentication and message encryption to PATROL developers. It includes a dynamically loaded (runtime) security module which encapsulates the PATROL Kerberos/GSS library calls.

key pair

A set of two cryptographic keys, one public and freely shared, one private and kept secret, used to encrypt and decrypt data. Synonym: public/private key pair.

KM

See Knowledge Module (KM).

Knowledge Module (KM)

A set of files from which a PATROL Agent receives information about resources running on a monitored computer. A KM file can contain the actual instructions for monitoring objects or simply a list of KMs to load. KMs are loaded by a PATROL Agent and a PATROL Console.

KMs provide information for the way monitored computers are represented in the PATROL interface, for the discovery of application instances and the way they are represented, for parameters that are run under those applications, and for the options available on object pop-up menus. A PATROL Console in the developer mode can change KM knowledge for its current session, save knowledge for all of its future sessions, and commit KM changes to specified PATROL Agent computers.

PATROL Agent

The core component of PATROL architecture. The agent is used to monitor and manage host computers and can communicate with the PATROL Console, a stand-alone event manager (PEM), PATROL Integration products, and SNMP consoles. From the command line, the PATROL Agent is configured by the pconfig utility; from a graphical user interface, it is configured by the xpconfig utility for Unix or the wpconfig utility for Windows.

PATROL Command Line Interface (CLI)

An interface program that you can access from the command line of a monitored computer and through which you can run some PATROL products and utilities. With the CLI, you can monitor the state of PATROL Agents remotely, execute PSL functions, and query and control events. The CLI is used in place of the PATROL Console when memory and performance constraints exist.

PATROL Console

The graphical user interface from which you launch commands and manage the environment monitored by PATROL. The PATROL Console displays all of the monitored computer instances and application instances as icons. It also interacts with the PATROL Agent and runs commands and tasks on each monitored computer. The dialog is event-driven so that messages reach the PATROL Console only when a specific event causes a state change on the monitored computer.

A PATROL Console with developer functionality can monitor and manage computer instances, application instances, and parameters; customize, create, and delete locally loaded Knowledge Modules and commit these changes to selected PATROL Agent computers; add, modify, or delete event classes and commands in the Standard Event Catalog; and define expert advice. A PATROL Console with operator functionality can monitor and manage computer instances, application instances, and parameters and can view expert advice but not customize or create KMs, commands, and parameters.

PATROL roles

In PATROL 3.x and earlier, a set of permissions that grant or remove the ability of a PATROL Console or PATROL Agent to perform certain functions. PATROL roles are defined in the PATROL User Roles file, which is read when the console starts.

PATROL Script Language (PSL)

A scripting language (similar to Java) that is used for generic system management and that is compiled and executed on a virtual machine running inside the PATROL Agent. PSL is used for writing application discovery procedures, parameters, recovery actions, commands, and tasks for monitored computers within the PATROL environment.

PSL	*See* PATROL Script Language (PSL).
public key infrastructure (PKI)	The protocols, services, and standards used by a certificate authority to manage public keys. Often a PKI is used by an organization or an enterprise to provide communications security within that enterprise.
setup command	A command that is initiated by the PATROL Console and run by the PATROL Agent when the PATROL Console connects or reconnects to the agent. For example, a setup command can initialize an application log file to prepare it for monitoring. PATROL provides some setup commands for computer classes. Only a PATROL Console with developer functionality can add or change setup commands.
signing	The actions that a certificate authority (CA) takes to create a valid digital certificate by first hashing the certificate contents and then signing the hash with the CA's private key.
secure socket layer (SSL) protocol	A standard protocol created by Netscape for secure message transmission in a network. It provides a cryptographic protocol for both mutual authentication and data protection of Internet communications.
startup command	*See* setup command.
trusted root certificate authority	The final certificate authority whose digital signature and certificate completes the validation of a digital certificate.
user profile	The PATROL Web Central specific information that is associated with a particular user. It corresponds directly to the user and is defined by the user back-end. The groups to which certain users belong are properties of that user.
user profile template	What you use to create your profile. It contains the default information in your user profile, but does not map to the user group.

Index

A

B

C

D

E

G

I

K

L

M

N

O

P

R

S

T

U

V

W

STOP!

IMPORTANT INFORMATION - DO NOT INSTALL THIS PRODUCT UNLESS YOU HAVE READ ALL OF THE FOLLOWING MATERIAL

By clicking the YES or ACCEPT button below (when applicable), or by installing and using this Product or by having it installed and used on your behalf, You are taking affirmative action to signify that You are entering into a legal agreement and are agreeing to be bound by its terms, EVEN WITHOUT YOUR SIGNATURE. BMC is willing to license this Product to You ONLY if You are willing to accept all of these terms. CAREFULLY READ THIS AGREEMENT. If You DO NOT AGREE with its terms, DO NOT install or use this Product; press the NO or REJECT button below (when applicable) or promptly contact BMC or your BMC reseller and your money will be refunded if by such time You have already purchased a full-use License.

SOFTWARE LICENSE AGREEMENT FOR BMC PRODUCTS

SCOPE. This is a legally binding Software License Agreement (**"License"**) between You (either an individual or an entity) and BMC pertaining to the original computer files (including all computer programs and data stored in such files) contained in the enclosed Media (as defined below) or made accessible to You for electronic delivery, if as a prerequisite to such accessibility You are required to indicate your acceptance of the terms of this License, and all whole or partial copies thereof, including modified copies and portions merged into other programs (collectively, the **"Software"**). **"Documentation"** means the related hard-copy or electronically reproducible technical documents furnished in association with the Software, **"Media"** means the original BMC-supplied physical materials (if any) containing the Software and/or Documentation, **"Product"** means collectively the Media, Software, and Documentation, and all Product updates subsequently provided to You, and **"You"** means the owner or lessee of the hardware on which the Software is installed and/or used. **"BMC"** means BMC Software Distribution, Inc. unless You are located in one of the following regions, in which case "BMC" refers to the following indicated BMC Software, Inc. subsidiary: (i) Europe, Middle East or Africa --BMC Software Distribution, B.V., (ii) Asia/Pacific -- BMC Software Asia Pacific Pte Ltd., (iii) Brazil -- BMC Software do Brazil, or (iv) Japan -- BMC Software K.K. **If You enter into a separate, written software license agreement signed by both You and BMC or your authorized BMC reseller granting to you the rights to install and use this Product, then the terms of that separate, signed agreement will apply and this License is void.**

FULL-USE LICENSE. Subject to these terms and payment of the applicable license fees, BMC grants You this non-exclusive License to install and use one copy of the Software for your internal use on the number(s) and type(s) of servers or workstations for which You have paid or agreed to pay to BMC or your BMC reseller the appropriate license fee. If your license fee entitles You only to a License having a limited term, then the duration of this License is limited to that term; otherwise this License is perpetual, subject to the termination provisions below.

TRIAL LICENSE. If You have not paid or agreed to pay to BMC or your BMC Reseller the appropriate license fees for a full use license, then, **NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS LICENSE**: (i) this License consists of a non-exclusive evaluation license ("Trial License") to use the Product for a limited time ("Trial Period") only for evaluation; (ii) during the Trial Period, You may not use the Software for development, commercial, production, database management or other purposes than those expressly permitted in clause (i) immediately above; and (iii) your use of the Product is on an ***AS IS*** basis, and **BMC, ITS RESELLERS AND LICENSORS GRANT NO WARRANTIES OR CONDITIONS (INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE) TO YOU AND ACCEPT NO LIABILITY WHATSOEVER RESULTING FROM THE USE OF THIS PRODUCT UNDER THIS TRIAL LICENSE.** If You use this Product for other than evaluation purposes or wish to continue using it after the Trial Period, you must purchase a full-use license. When the Trial Period ends, your right to use this Product automatically expires, though in certain cases You may be able to extend the term of the Trial Period by request. Contact BMC or your BMC reseller for details.

TERM AND TERMINATION. This License takes effect on the first to occur of the date of shipment or accessibility to You for electronic delivery, as applicable (the **"Product Effective Date"**). You may terminate this License at any time for any reason by written notice to BMC or your BMC reseller. This License and your right to use the Product will terminate automatically with or without notice by BMC if You fail to comply with any material term of this License. Upon termination, You must erase or destroy all components of the Product including all copies of the Software, and stop using or accessing the Software. Provisions concerning Title and Copyright, Restrictions (or Restricted Rights, if You are a U.S. Government entity) or limiting BMC's liability or responsibility shall survive any such termination.

TITLE AND COPYRIGHT; RESTRICTIONS. All title and copyrights in and to the Product, including but not limited to all modifications thereto, are owned by BMC and/or its affiliates and licensors, and are protected by both United States copyright law and applicable international copyright treaties. You will not claim or assert title to or ownership of the Product. To the extent expressly permitted by applicable law or treaty notwithstanding this limitation, You may copy the Software only for backup or archival purposes, or as an essential step in utilizing the Software, but for no other purpose. You will not remove or alter any copyright or proprietary notice from

copies of the Product. You acknowledge that the Product contains valuable trade secrets of BMC and/or its affiliates and licensors. Except in accordance with the terms of this License, You agree (a) not to decompile, disassemble, reverse engineer or otherwise attempt to derive the Software's source code from object code except to the extent expressly permitted by applicable law or treaty despite this limitation; (b) not to sell, rent, lease, license, sublicense, display, modify, time share, outsource or otherwise transfer the Product to, or permit the use of this Product by, any third party; and (c) to use reasonable care and protection to prevent the unauthorized use, copying, publication or dissemination of the Product and BMC confidential information learned from your use of the Product. **You will not export or re-export any Product without both the written consent of BMC and the appropriate U.S. and/ or foreign government license(s) or license exception(s).** Any programs, utilities, modules or other software or documentation created, developed, modified or enhanced by or for You using this Product shall likewise be subject to these restrictions. BMC has the right to obtain injunctive relief against any actual or threatened violation of these restrictions, in addition to any other available remedies. Additional restrictions may apply to certain files, programs or data supplied by third parties and embedded in the Product; consult the Product installation instructions or Release Notes for details.

LIMITED WARRANTY AND CONDITION. If You have purchased a Full-Use License, BMC warrants that (i) the Media will be, under normal use, free from physical defects, and (ii) for a period of ninety (90) days from the Product Effective Date, the Product will perform in substantial accordance with the operating specifications contained in the Documentation that is most current at the Product Effective Date. BMC's entire liability and your exclusive remedy under this provision will be for BMC to use reasonable best efforts to remedy defects covered by this warranty and condition within a reasonable period of time or, at BMC's option, either to replace the defective Product or to refund the amount paid by You to license the use of the Product. BMC and its suppliers do not warrant that the Product will satisfy your requirements, that the operation of the Product will be uninterrupted or error free, or that all software defects can be corrected. This warranty and condition shall not apply if: (i) the Product is not used in accordance with BMC's instructions, (ii) a Product defect has been caused by any of your or a third party's malfunctioning equipment, (iii) any other cause within your control causes the Product to malfunction, or (iv) You have made modifications to the Product not expressly authorized in writing by BMC. No employee, agent or representative of BMC has authority to bind BMC to any oral representations, warranties or conditions concerning the Product. **THIS WARRANTY AND CONDITION IS IN LIEU OF ALL OTHER WARRANTIES AND CONDITIONS. THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING THOSE OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS LICENSE OR ANY PRODUCT LICENSED HEREUNDER. THIS PARAGRAPH SHALL NOT APPLY TO A TRIAL LICENSE.** Additional support and maintenance may be available for an additional charge; contact BMC or your BMC reseller for details.

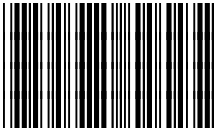
LIMITATION OF LIABILITY. Except as stated in the next succeeding paragraph, BMC's and your BMC reseller's total liability for all damages in connection with this License is limited to the price paid for the License. **IN NO EVENT SHALL BMC BE LIABLE FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE USE OF THIS PRODUCT (SUCH AS LOSS OF PROFITS, GOODWILL, BUSINESS, DATA OR COMPUTER TIME, OR THE COSTS OF RECREATING LOST DATA), EVEN IF BMC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Some jurisdictions do not permit the limitation of consequential damages so the above limitation may not apply.

INDEMNIFICATION FOR INFRINGEMENT. BMC will defend or settle, at its own expense, any claim against You by a third party asserting that your use of the Product within the scope of this License violates such third party's patent, copyright, trademark, trade secret or other proprietary rights, and will indemnify You against any damages finally awarded against You arising out of such claim. However, You must promptly notify BMC in writing after first receiving notice of any such claim, and BMC will have sole control of the defense of any action and all negotiations for its settlement or compromise, with your reasonable assistance. BMC will not be liable for any costs or expenditures incurred by You without BMC's prior written consent. If an order is obtained against your use of the Product by reason of any claimed infringement, or if in BMC's opinion the Product is likely to become the subject of such a claim, BMC will at its option and expense either (i) procure for You the right to continue using the product, or (ii) modify or replace the Product with a compatible, functionally equivalent, non-infringing Product, or (iii) if neither (i) nor (ii) is practicable, issue to You a pro-rata refund of your paid license fee(s) proportionate to the number of months remaining in the 36 month period following the Product Effective Date. This paragraph sets forth your only remedies and the total liability to You of BMC, its resellers and licensors arising out of such claims.

GENERAL. This License is the entire understanding between You and BMC concerning this License and may be modified only in a mutually signed writing between You and BMC. If any part of it is invalid or unenforceable, that part will be construed, limited, modified, or, severed so as to eliminate its invalidity or unenforceability. This License will be governed by and interpreted under the laws of the jurisdiction named below, without regard to conflicts of law principles, depending on which BMC Software, Inc. subsidiary is the party to this License: (i) BMC Software Distribution, Inc. - the State of Texas, U.S.A., (ii) BMC Software Distribution, B.V. - The Netherlands, (iii) BMC Software Asia Pacific Pte Ltd. -- Singapore (iv) BMC Software do Brazil -- Brazil, or (v) BMC Software K.K. -- Japan. Any person who accepts or signs changes to the terms of this License promises that they have read and understood these terms, that they have the authority to accept on your behalf and legally obligate You to this License. Under local law and treaties, the restrictions and limitations of this License may not apply to You; You may have other rights and remedies, and be subject to other restrictions and limitations.

U.S. GOVERNMENT RESTRICTED RIGHTS. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in FAR Section 52.227-14 Alt. III (g)(3), FAR Section 52.227-19, DFARS 252.227-7014 (b) or DFARS 227.7202, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Notes



17344